UNIVERSIDAD PABLO DE OLAVIDE DE SEVILLA, ESPAÑA.

FACULTAD DE DERECHO
DEPARTAMENTO DE DERECHO PRIVADO

TESIS DOCTORAL:

La protección de datos de carácter personal en la gestión de los recursos humanos de la empresa.

Presentada por OLGA GARCÍA COCA para optar al grado de Doctora en Ciencias Jurídicas y Políticas por la Universidad Pablo de Olavide de Sevilla.

Dirigida por:
DR. SANTIAGO GONZÁLEZ ORTEGA

Depositada en Sevilla, a 12 de mayo de 2016.

A mis padres, Jaime y Mª Angeles
por ser mi ejemplo y ayuda cada día.
A mi marido, Francisco
por ser mi apoyo incondicional en la vida.
A mis hijos, Álvaro y Manuel
por ser mi alegría y el sentido de mi caminar.

"(…) cuando el Derecho se enfrenta al problema práctico de definir un nuevo derecho que proteja al propio ser humano, en realidad se está enfrentando a un nuevo tipo de abuso."

*(*M. Marván Laborde*)*[1]*.*

[1] MARVAN LABORDE, M.: "Prólogo" de la obra de DÁVARA RODRÍGUEZ, I.: *Hacia la estandarización de la protección de datos de carácter personal,* La Ley, 2011, pág. 20.

AGRADECIMIENTOS

A mi maestro, Santiago González Ortega, por la orientación y ayuda que me ha brindado para la realización de esta tesis, por creer en mí, y por tantos ánimos a lo largo de este tiempo.

A todos mis compañeros del Área de Derecho del Trabajo y de la Seguridad Social de la Universidad Pablo de Olavide por conseguir sacar el lado positivo de esta etapa. Al equipo del departamento de Derecho Privado de la Universidad Pablo de Olavide por su apoyo y consejos de gran valor, especialmente y en particular a Juan Pablo Pérez Velázquez, María Serrano, Reyes Sánchez Leria, Lucia Vázquez-Pastor, y en general a todos. A Laura García Álvarez por su alegría y por demostrar ser mucho más que una compañera de trabajo. Y a tantos otros compañeros y amigos de la UPO que están comprometidos para lograr que la Universidad sea un lugar de encuentro y de intercambio de culturas diversas.

A Maria Paola Aimo de la Universitá degli studio di Torino (Italia) y a Marco Lai del Centro di Studio Nazionale (CSIL) de Florencia (Italia), por su amable colaboración y su ejemplo en la defensa de los derechos fundamentales del trabajador.

A todos los que me han cuidado, animado y acompañado en estos años. Principalmente, a mis hermanos Irene y Jaime por estar siempre ahí y por hacerme ver lo realmente valioso de la vida; a mis abuelos por su forma de afrontar la vida y los buenos consejos recibidos; a mis suegros por su ayuda en la difícil conciliación laboral y familiar; a mis sobrinos, que me recuerdan lo que de verdad merece la pena; y a toda mi familia y amigos por su comprensión y ánimo durante este tiempo.

A la Universidad Pablo de Olavide por verme crecer en lo profesional y personal, por ser fuente de sabiduría y, sobre todo, por darme la oportunidad de iniciar mi carrera investigadora y culminar mis estudios de doctorado.

En definitiva a todos los hombres y mujeres que intentan hacer de la sociedad un espacio en dónde la libertad de uno no invada la de otros, y procuran que el respeto y la paz sean el pilar de nuestro día a día. .

TABLA DE CONTENIDOS

ABREVIATURAS

AEAT: Agencia Estatal de Administración Tributaria.

AEPD: Agencia Española de Protección de Datos de Carácter Personal.

APDCM: Agencia de Protección de Datos de la Comunidad de Madrid.

BOE: Boletín Oficial del Estado.

BOCG: Boletín Oficial de las Cortes Generales.

Carta de DDFF: Carta de Derechos Fundamentales de la Unión Europea.

CCC: Código Cuenta Cotización.

CE: Constitución Española.

CEDH: Convenio Europeo de Derechos Humanos.

CENDOJ: Centro de Documentación del Poder Judicial.

CNIL: Comisión Nacional de Informática y Libertades.

Convenio Europeo de Derechos Humanos: Convenio para la protección de los derechos humanos y de las libertades fundamentales.

Convenio 108 de Europa; Convenio 108 de Europa para la protección de las personas físicas en lo que respecta al tratamiento automatizado de sus datos personales.

CV: Curriculum Vitae.

Directiva 95/46/CE: Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

DOUE: Diario Oficial de la Unión Europea.

DUDH: Declaración Universal de Derechos Humanos.

ET: Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

ETC; Espacio Telemático Común.

EURES; Red Eures de empleo.

FNMT: Fábrica Nacional de Moneda y Timbre.

GT 29: Grupo de trabajo de la Comisión Europea del art. 29.

Instrucción 1/1998: Instrucción 1/1998 de la AEPD sobre el ejercicio de los derechos de acceso, rectificación y cancelación.

LAECSP: Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

LO: Ley Orgánica.

Ley 1/1982: Ley 1/1982 de 5 de mayo reguladora de la protección civil del derecho al honor a la intimidad personal y familiar y a la propia imagen.

LETT: Ley 14/1994, de 1 de junio, reguladora de las Empresas de Trabajo Temporal.

Ley 36/2011: Ley 36/2011, de 10 de octubre, reguladora de la Jurisdicción Social.

LOLS: Ley 2/1985, de 2 de agosto, de Libertad Sindical.

LOPD: Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

LORTAD: Ley Orgánica 5/1992, de 29 de octubre de regulación del tratamiento automatizado de los datos de carácter personal.

Ley 10/1994: Ley 10/1994 de 19 de mayo sobre medidas urgentes de fomento de la ocupación.

Ley de Empleo: Real Decreto Legislativo 3/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley de Empleo.

LGSS: Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social.

LJS: Ley 36/2011, de 10 de octubre, reguladora de la Jurisdicción Social.

MCSS: Mutuas colaboradoras con la Seguridad Social.

MTAS: Ministerio de Trabajo y Asuntos Sociales.

Orden ESS/484/2013: Orden ESS/484/2013, de 26 de marzo, por la que se regula el Sistema de remisión electrónica de datos en el ámbito de la Seguridad Social

RD: Real Decreto.

RD 1332/1994: RD 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los datos de carácter personal.

RDL 17/1977: Real Decreto Ley 17/1977, de 4 de marzo, sobre las relaciones de trabajo.

RDLOPD: RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

RD 735/1995: RD 735/1995, de 5 de mayo, por el que se regulan las agencias de colocación sin fines lucrativos y los servicios integrados para el empleo.

RDL 10/2010: RDL 10/2010, de 16 de junio, de medidas urgentes para la reforma del mercado de trabajo.

RD 1796/2010: RD 1796/2010, de 30 de diciembre, por el que se regulan las agencias de colocación.

RD 7/2015: RD 7/2015, de 16 de enero, por el que se aprueba la Cartera Común de Servicios del Sistema Nacional de Empleo.

RGPD: Reglamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

RMS: Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.

SAE: Servicio Andaluz de Empleo.

SAN; Sentencia de la Audiencia Nacional.

SEPE: Servicio Estatal Público de Empleo.

SEPCCAA: Servicio de Empleo Comunidades Autónomas.

SISPE: Sistema de Información de los Servicios Públicos de Empleo.

SNE: Sistema Nacional de empleo.

STC 292/2000: Sentencia 292/2000 de 30 de noviembre del Tribunal Constitucional.

STJCE: Sentencia del Tribunal de Justicia de la Comunidad Europea.

TEDH: Tribunal Europeo de Derechos Humanos.

TICS: Tecnologías de la información y la comunicación.

TJCE: Tribunal de Justicia de la Comunidad Europea.

TSJ: Tribunal Superior de Justicia.

TS: Tribunal Supremo.

UE: Unión Europea.

INTRODUCCIÓN

"(…) en el pasado ningún Estado tenía el poder suficiente para someter a todos sus ciudadanos a una vigilancia constante"

George Orwell[2].

Las relaciones de trabajo actuales y los efectos que la gestión de los recursos humanos de la empresa puede tener respecto al derecho a la protección de datos de carácter personal de los trabajadores, ha supuesto la necesidad de estudiar la magnitud y los retos jurídicos que plantea en el panorama empresarial el respeto a la privacidad de los empleados. Por ello, se ha considerado necesario analizar la protección de datos del trabajador, desde una doble perspectiva; por un lado, el procesamiento de los datos de aquellas personas que se encuentren buscando empleo; y por otro, el estudio del tratamiento de la información personal de los trabajadores durante el desarrollo de la actividad laboral.

Dada las repetidas ocasiones en las que se ha tratado la acepción datos de carácter personal se debe, en estas páginas introductorias, concretar, atendiendo a lo establecido en la LOPD, su definición: *"cualquier información concerniente a personas físicas identificadas o identificables"*[3], concepto que es matizado y ampliado cuando se define como "*cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"*[4]. Cierto es que, la Ley 15/1999 de 13 de diciembre de protección de datos de carácter personal[5] no define que debe entenderse por persona identificable acudiendo, entonces, a lo establecido en el art. 2 a) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre

[2] ORWELL, G.: *Teoría y práctica del colectivismo oligárquico*, Edic. Destino, vol. 54, 2004, pág. 20.
[3] Art. 3. a) LOPD.
[4] Art. 5.1. f) RDLOPD.
[5] BOE núm.298 de 14 de diciembre de 1999.

circulación de estos datos[6], la cual establece que: *"se considera identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*".

En este contexto, se hace preciso distinguir el tipo de datos que va a necesitar el empresario para poder llevar a cabo sus funciones relacionadas con la gestión de los recursos humanos, pues existen determinadas informaciones de los trabajadores que gozan de una protección especial en la normativa sobre protección de datos de carácter personal[7], como son los datos relativos a su salud, ideología, religión, creencias, vida sexual, etc[8]. Concluyendo que la información, tanto de ciudadanos que quieren acceder a un puesto de trabajo como la que recoge el empresario de sus trabajadores en la empresa, constituye lo que la legislación sobre protección de datos ha catalogado como dato de carácter personal.

Ahora bien, una vez precisado el concepto de dato de carácter personal se ha decidido acotar el objeto de estudio de esta tesis doctoral a aquellos

[6] Diario Oficial n° L 281 de 23 de noviembre de 1995. Sin embargo, con fecha 27 de abril de 2016 se ha aprobado de forma definitiva el Reglamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de protección de datos), (DOUE nº L 119/1 de 4 de mayo de 2016). No obstante, la derogación de la Directiva 95/46/CE está prevista para dos años después de la entrada en vigor del Reglamento, concretamente el RGPD se aplicará a partir del 25 de mayo de 2018 (art. 99). Sin embargo, a lo largo del presente trabajo se ha ido haciendo referencia a las novedades introducidas por el RGPD, teniendo en cuenta las que más pueden afectar a la protección de datos de los trabajadores, sin hacer un estudio exhaustivo del mismo, ya que la Directiva 95/46/CE se encuentra actualmente en vigor.

[7] Clasificación de datos de carácter personal extraída del formulario NOTA (instrumento de notificación de los ficheros de datos a la AEPD); datos identificativos, datos especialmente protegidos, detalles de empleo, datos relativos a características personales o a circunstancias sociales, datos profesionales o académicos etc.

[8] Sobre el concepto de dato de carácter personal: PIÑAR MAÑAS, J.L.: "Concepto de dato de carácter personal" en VV.AA. *Comentarios a la Ley Orgánica de protección de datos de carácter personal*, Civitas, Thomson Reuters, 2010, pp.193-195; LESMES SERRANO, C.: "Comentario al artículo 3", en el libro colectivo dirigido por él mismo La Ley de Protección de datos. Análisis y Comentario de su jurisprudencia, Lex Nova, 2008, pág. 110; COLLADA GARCÍA-LAJARA, E.: Protección de datos de carácter personal. Legislación, comentarios y jurisprudencia. Comares, 2001, pp.11-13, 22-26.

aspectos referidos al tratamiento[9] de la información personal de los trabajadores, el cual se deduce del registro de esos datos de los trabajadores en los distintos soportes con los que cuenta la empresa y de las oportunas cesiones que se puedan hacer con motivo de las diferentes gestiones relacionadas con la administración de la plantilla de trabajadores. Sobre este aspecto, relativo a la cesión de datos, cabe hacer un inciso pues la LOPD cuando define lo que se entiende por tratamiento incluye también a la cesión. Pero, a pesar de ello, se ha estimado hacer un estudio de esta figura aparte para así hacer un análisis de la comunicación de datos a terceros, ya que realmente es lo que va a efectuar el empresario para poder administrar la selección de personal y los recursos humanos de su centro de trabajo.

Lógicamente, el procesamiento de estas informaciones adquiere más notoriedad a raíz de la implantación de las TICS en la empresa, las cuales permiten que existan de forma más rápida y eficaz el almacenamiento de los datos de los empleados y un mayor trasvase de información entre empleados, trabajadores y otros organismos colaboradores en la gestión del personal de la empresa. Ahora bien, el uso de estos mecanismos tecnológicos, en ocasiones, ha lesionado el derecho a la protección de datos de los trabajadores al no seguir lo establecido en la LOPD a la hora de registrar su información empresarial en los ficheros empresariales[10], teniendo en cuenta que la ubicación de informaciones en soportes informáticos y su tratamiento o comunicación es tangible para un mayor número de interlocutores, que si ésta estuviera en un fichero manual. Por este motivo, y dado que en la actualidad lo lógico es que el empresario proceda a la informatización de todos los datos de los trabajadores, se ha considerado preciso abordar la problemática que puede acarrear el manejo de estas bases de datos en los soportes tecnológicos de la

[9] Art. 3 c) de la LOPD: *"Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".*

[10] COLÁS NEILAS E.: *Derecho fundamentales del trabajador en la era digital: una propuesta metodológica para su eficacia*, Bomarzo, 2012, pág. 108; LOY, G.: "El dominio ejercido sobre el trabajador" *Revista Relaciones Laborales*, núm. 19-20, 2005, pág. 61.

empresa, tanto a la hora de seleccionar un trabajador para una concreta oferta de empleo como para organizar su plantilla dentro ya del centro de trabajo[11].

De este modo, se puede decir que desde un punto de vista legal se han posicionado dos derechos importantes relacionados. Por un lado, el derecho del empleador a organizar su empresa libremente[12] y ejercer, una vez se haya registrado la información de los demandantes de empleo y de los trabajadores, una cierta disposición de esos datos vinculados a sus labores empresariales y organizativas; y por otra parte, el derecho del trabajador a que los datos obrantes en los ficheros de la empresa o los obtenidos por otro mecanismos[13], necesarios para la administración de los recursos humanos, sean tratados de forma diligente, sin que ese tratamiento suponga un atentado en su privacidad.

Varios fundamentos han sido claves para elección de este tema de investigación y el uso de la siguiente perspectiva de análisis: a) su relevancia y actualidad jurídica, dada la incompleta respuesta que la normativa sobre protección de datos otorga a la salvaguarda de este derecho en el panorama de las relaciones laborales y la utilidad social que tendría una regulación vinculante encaminada a la resolución de los conflictos que se generan en el ámbito empresarial; b) la dificultad existente a la hora de distinguir el derecho a la protección de datos del derecho a la intimidad en el ámbito de las relaciones de trabajo; c) la aplicación de los principios de la protección de datos en los distintos mecanismos de intermediación laboral estudiados, siendo deficiente en aquellas plataformas de búsqueda de empleo, redes sociales, sistemas de almacenamiento masivo de datos etc.; d) el procesamiento de más datos de los necesarios en el momento de la contratación del trabajador y durante el

[11] PRADAS MONTILLA, R.: "Organización del trabajo y nuevas tecnologías" *Documentación Laboral*, núm.53, 1997.pág 15 y ss.; RODRÍGUEZ ESCANCIANO, S. Y FERNÁNDEZ DOMÍNGUEZ, J.J.: *Utilización y control de datos laborales automatizados* AEPD, 1997, pp.19-21; MERCADER UGUINA, J.: *Derecho del Trabajo. Nuevas Tecnologías y Sociedad de la Información.* Lex Nova, 2002, págs. 49 y ss.; GONZÁLEZ ORTEGA, S.: "La informática en el seno de la empresa. Poderes del empresario y condiciones de trabajo" en VV.AA.: *Nuevas Tecnologías de la información y comunicación en el Derecho del Trabajo,* Bomarzo, 2004, pp. 21-22.

[12] Art. 38 CE; *"Se reconoce la libertad de empresa en el marco de la economía de mercado. Los poderes públicos garantizan y protegen su ejercicio y la defensa de la productividad, de acuerdo con las exigencias de la economía general y, en su caso, de la planificación."*

[13] Mecanismos de control de entrada al centro de trabajo, supervisión del ordenador y del correo electrónico, conocimiento de datos relativos a la afiliación sindical para el descuento cuota sindical, comunicaciones de datos a través de medios informático etc.

transcurso de la relación de trabajo, analizando si es obligatorio aportar más informaciones de las realmente precisas para ese cometido; e) y por último, la mala praxis empresarial habida para la supresión de los ficheros con datos de los trabajadores, una vez finalizado el contrato de trabajo.

La realización de este estudio, con las características y fines señalados, ha exigido un *modus operandi*[14] basado en primer lugar en el examen técnico-jurídico de la normativa sobre protección de datos de carácter personal y la normativa comunitaria sobre el tema para poder aplicar lo allí contenido a la utilización y tratamiento de datos de los trabajadores sitos en los ficheros empresariales. En este sentido, prepondera el espíritu de la observación de los supuestos planteados fundamentada no sólo en su descripción, sino en la adecuación a estas legislaciones para conocer el grado de cumplimiento por parte del empresario cuando va a procesar datos de sus empleados.

Como consecuencia de la carencia de una norma sectorial, que regule la problemática de la protección de datos del trabajador y para acceder a un conocimiento más acabado y certero del tema, ha sido inevitable complementar las referencias normativas los informes y conclusiones realizados por la Agencia Española de Protección de datos[15], así como, los documentos redactados por el Grupo de Trabajo del art. 29 (GT 29)[16].

---

[14] Según WITKER; "*la curiosidad, la observación, la abstracción, la comprobación y la tesis o producto científico son los elementos metodológicos preliminares para realizar una investigación jurídica*" en *Metodología de la Enseñanza del Derecho,* pp. 112-118. Para ALONSO GARCÍA, M. por método, en Derecho del Trabajo, hay que entender "*el procedimiento necesario para llegar a conocer una cosa verdaderamente, es decir, el camino imprescindible para acceder a un adecuado conocimiento del Derecho"* en. *El método jurídico y su aplicación al Derecho del Trabajo*, Reus, 1959, pág.4.

[15] Ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada que tiene como función principal velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

[16] Grupo de trabajo creado en el seno de la Comisión Europea por la Directiva 95/46/CE tiene carácter de órgano consultivo independiente y está integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea - que realiza funciones de secretariado-. Asimismo, los Estados candidatos a ser miembros de la Unión y los países miembros del EEE acuden a las reuniones del GT 29 en condición de observadores. La Agencia Española de Protección de Datos forma parte del mismo desde su inicio, en febrero de 1997.

Una vez culminada esta fase de conocimiento de material normativo y documental, ha sido indispensable hacer uso de otros instrumentos para conocer la realidad social actual y la inobservancia que se presenta, en algunos sectores, de la legislación que custodia los datos personales. Para ello, se ha utilizado el método empírico-jurídico encaminado a recolectar información a través de encuestas, entrevistas, estudio de las políticas de privacidad de empresas, páginas web, redes sociales etc.[17]

Por último, se ha realizado una investigación cualitativa teniendo presente la hipótesis inicial pero sin descuidar las preguntas y sospechas que se pueden desarrollar antes, durante o después de la recolección y el examen de información. Por ello, lo que se ha procurado es asimilar la realidad de la protección de datos de carácter personal extrayendo e interpretando los fenómenos de acuerdo con las personas implicadas, en este caso los desempleados y los trabajadores[18].

Con el uso de esta metodología se ha demostrado la necesidad de combinar distintos métodos[19] para así poder lograr el objetivo planteado con cierta profundidad, dando respuesta a las problemáticas sugeridas[20], siendo ésta la más adecuada teniendo en cuenta la ausencia de una norma sectorial que regule la casuística generada por el tratamiento de datos de los trabajadores en la empresa.

Partiendo de estos interrogantes y líneas argumentales, organizaremos el trabajo en cuatro bloques o capítulos.

[17] WITKER, J.: La investigación jurídica, UNAM, 2009, pp. 50-51.
[18] DENZIN, N.K. Y LINCOLN, Y.S.: *Handbook of Qualitative Research,* London: Sage Publications, 2000, pp. 1-28.
[19] Esta forma de realizar un trabajo de investigación ha sido reiterada por la doctrina así, ALONSO GARCÍA, M.: *El método jurídico y su aplicación al Derecho del Trabajo*, Reus, 1959, pág. 106; VALLET DE GOYTISOLO, J.: *Metodología Jurídica*, Civitas, Madrid, 1988, págs. 65-66 y 155-156.
[20] Siguiendo a JAVILLIER Y AUVEGNON: *"No hay investigación sin problemática, sin presupuesto crítico"* "Elements por un bilan sur la rcherche en droit du travail". *Revista Droit Social*, núm. 3, 1990, pág. 212.

El primero de ellos, ha abordado la problemática relativa al cuadro normativo. Pero, antes de matizar las vicisitudes del marco legal de la protección de datos se ha considerado hacer una breve referencia al derecho europeo en la materia, ya que la normativa de protección de datos, en vigor en nuestro país, constituye un reflejo casi idéntico de lo contenido en la citada Directiva 95/46/CE. En esta extensión, la transposición de la normativa europea a nuestro derecho interno propició la promulgación de la LOPD y más tarde la del RD 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[21], cumpliendo de esta forma con el mandato constitucional contenido en el art. 18.4 CE[22]. Como es sabido, la configuración del derecho a la protección de datos como derecho fundamental, independiente y autónomo del derecho a la intimidad tiene un enfoque jurisprudencial adquiriendo esta categoría a raíz de lo establecido por el Tribunal Constitucional[23], aspecto que ha merecido ser tratado en este primer capítulo debido a la trascendencia que tiene esa diferenciación, para su análisis en el panorama laboral.

En este orden, se ha analizado el ámbito de aplicación de la normativa sobre protección de datos en los aspectos que se van a tratar a lo largo de esta tesis, haciendo una descripción de los principios y derechos que rigen la defensa de los datos de carácter personal, para realizar una interpretación extensiva de su estudio no sólo a los procesos de selección de personal, previos a cualquier estado de contratación laboral, sino también a la repercusión que tiene la protección de la información de los trabajadores durante el desarrollo de la prestación de trabajo, para finalmente abordar su exégesis en la extinción del contrato laboral. Quizás los principios que más influencia tienen respecto al objeto de este estudio sean el de calidad, información, y consentimiento, unidos al de seguridad, pues son los que tendrán que respetarse para realizar un adecuado tratamiento de cualquier

[21] BOE núm. 17 de 19 de enero de 2008.
[22] Art. 18.4 de la CE: *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."*
[23] Las sentencias del Tribunal Constitucional 290 y 292 de 30 de noviembre de 2000, representan la culminación en el reconocimiento del derecho fundamental a la protección de datos de carácter personal puesto que, existen sentencias precedentes que ya hacían alusión a la posible admisión de este aspecto pero sin concretar definitivamente la misma.

información de tipo personal. En otro punto, se ha considerado importante hacer referencia a las garantías, representadas en los derechos de acceso, rectificación, cancelación y oposición, que la normativa dispensa a cualquier ciudadano y también, por tanto, a los trabajadores cuando observan alguna vulneración de su derecho a la protección de datos.

Para terminar de tratar la configuración del derecho a la protección de datos, se ha hecho mención expresa a las obligaciones que tiene el empresario (en el acceso al empleo o durante el desarrollo de la prestación laboral), en aras de cumplir con la salvaguarda de este derecho. En consecuencia, descrito el cuadro normativo y la descripción de los aspectos que más pueden incidir en las relaciones de trabajo, se hace necesario atender a la configuración de las instituciones de control existentes que pueden establecer requisitos para tratar los datos de carácter personal, sin tener que perjudicar a los trabajadores así como procurar su protección imponiendo sanciones de carácter administrativo a los empresarios que hagan un uso indebido de la información personal de sus empleados.

En este marco, se ha tratado la estructura del primero de los problemas referidos, es decir, el respeto del derecho a la protección de datos de carácter personal en los procesos de acceso al empleo. Como se ha comentado, en las relaciones previas a la contratación laboral, el ciudadano pretende flexibilizar la búsqueda de empleo acudiendo a empresas especializadas en esta actividad o dirigiéndose a los servicios de recursos humanos existentes en las propias empresas que ofertan puestos de trabajo[24]. Debido a la proliferación de empresas que funcionan como intermediadoras laborales es preciso acudir a la definición que establece el art. 31 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley de empleo[25]; *"La intermediación laboral es el conjunto de*

[24] El tratamiento de datos de los candidatos al empleo realizado por las empresas con servicios propios de recursos humanos es idéntico al realizado por los mecanismos de intermediación laboral, presentando diferencias a la hora de cumplimentar el contrato de trabajo, ya que es la empresa la que lo formaliza y tampoco necesita que le cedan los datos de los futuros trabajadores pues ya están registrados en sus bases de datos al ser ellas las que realizan la selección de personal.
[25] BOE núm. 255 de 24 de octubre de 2015.

acciones que tienen por objeto poner en contacto las ofertas de trabajo con los trabajadores que buscan un empleo, para su colocación. La intermediación laboral tiene como finalidad proporcionar a los trabajadores un empleo adecuado a sus características y facilitar a los empleadores los trabajadores más apropiados a sus requerimientos y necesidades."

Teniendo en cuenta esta definición[26], se ha delimitado de manera específica los mecanismos de intermediación más utilizados por los ciudadanos[27] para observar, en una segunda instancia, si estos medios realizan tratamiento de datos de los demandantes de empleo cumpliendo lo previsto en la LOPD. Ahora bien, se ha hecho necesario distinguir los tratamientos de datos que puede hacer una empresa de trabajo temporal y una agencia de colocación o el propio servicio de empleo, pues la funcionalidad de estas entidades tiene alguna diferencia que se comentará a lo largo de este estudio. También ha sido preciso concretar aquellos procesamientos de datos que desvirtúan cualquier proceso de selección de personal debido a la poca o ninguna justificación que tiene realizarlos para poder acreditar la capacidad de ese trabajador.

De otra parte, se ha considerado hacer acerca de la incursión de los medios tecnológicos en las empresas intermediadoras, lo que ha promovido nuevos retos para la mediación laboral pues la existencia de un espacio de intercambio de información en la red, que puede ser consultado de forma privada o pública por los agentes mediadores de empleo, se convierte en un instrumento de colaboración en la tarea de buscar candidatos para las ofertas

[26] Sobre el concepto de intermediación laboral: SÁNCHEZ-RODAS NAVARRO, C.: "La orientación e intermediación directa en el empleo" *Revista Temas Laborales*, núm.125, 2014, pp.104-105; ALZAGA RUIZ, I.: Intermediación laboral y formación profesional, *Revista del Ministerio de Empleo y Seguridad Social,* núm.100, 2012, pp. 69-70; GARCÍA FERNÁNDEZ, M.: "El artículo 20. Concepto" en VV.AA.: *El derecho del empleo. Estudio sistemático de la Ley 56/2003, de 16 de diciembre, de Empleo*. Comares, 2011, págs.466 y ss.; PRADOS DE REYES, F. Y MOLINA MARTÍN, A.M.: "Nuevos criterios para la ordenación de la intermediación laboral" *Revista de Derecho Social*, núm.54, 2011, pp.47-49; RAMÍREZ GONZÁLEZ, L.M.: "Contexto normativo y legal de la intermediación laboral en España y Andalucía" *Trabajo: Revista Andaluza de relaciones laborales*, núm. 24, 2011, pp.95-96.

[27] Según el art. 31 de la Ley de Empleo: *"A efectos del Sistema Nacional de Empleo, la intermediación en el mercado de trabajo se realizará a través de: a) Los servicios públicos de empleo. b) Las agencias de colocación. c) Aquellos otros servicios que reglamentariamente se determinen para los trabajadores en el exterior."*

de empleo que promocionan. Es por ello, por lo que se ha estimado estudiar su implantación no sólo en las empresas de intermediación, sino también su configuración como un mecanismo que por sí mismo puede actuar como medio de interrelación entre candidatos y ofertas de empleo (redes sociales[28], buscadores de empleo, informatización en los servicios de empleo público, software de análisis de datos, etc.). La captación de datos a través de estos instrumentos tecnológicos, traducidos en la eficacia de la red de comunicación que se establece con internet, ha permitido que en los procesos de selección se comuniquen y se consiga más datos del futuro trabajador que los imprescindibles para efectuar una correcta distinción entre un candidato u otro y justificar así, cuál se adapta mejor al puesto ofertado.

La forma en la que el encargado de realizar la selección de personal recoge esa información constituye un tratamiento de datos de carácter personal debido, principalmente, a la propia naturaleza del sistema que almacena directamente, en las bases de datos de la empresa (cloud computing, mecanismos de almacenamiento de información y gestión de los servicios públicos de empleo etc), información de los empleados y también al sometimiento de estos datos a programas informáticos determinados que analicen datos sobre la personalidad de los trabajadores (sistema experto Sigmund), aspectos que deben respetar lo contenido en la LOPD.

Obviamente y como consecuencia de la implantación de las TICS, en las propias páginas web de las agencias de intermediación se encuentran apartados en los que se podrá enviar el CV o, incluso, formularios habilitados para la inserción de la información identificativa y profesional de los candidatos al empleo. Además, existen muchos buscadores web en los que las empresas de intermediación o directamente la entidad que ofrece el empleo anuncian su oferta de trabajo, para que inserten sus datos en ellas aquellas personas que

[28] En este ámbito, hay que tener presente que el simple hecho de tener una cuenta abierta en una red social, tipo Facebook, Twitter, Tuenti etc., no significa que la información allí contenida pueda ser valorada para profundizar sobre la personalidad y aficiones del solicitante de empleo, pues esos datos al proceder de una red social no profesional no serían objetivos a efectos de evaluar la aptitud de esa persona para desempeñar una determinada actividad en la empresa.

crean cumplir con las características expuestas en el anuncio. Ahora bien, para poder fijar el cumplimiento de la normativa de protección de datos por parte de estos medios establecidos en la web, se ha hecho imprescindible observar las políticas de privacidad[29] expuestas en los portales webs de estas empresas.

La última parte de este capítulo se ha dedicado al estudio de la transferencia internacional de datos como mecanismo de intermediación laboral, como consecuencia de la internacionalización en la búsqueda de empleo. Esta universalización, concebida como una alternativa para aquellos desempleados que quieren ampliar el radio de búsqueda efectiva de trabajo a otros países, tiene su más fiel representación en la posibilidad que internet otorga a las empresas de publicar su anuncio y que pueda ser visto por cualquier persona independientemente del lugar en dónde se encuentre.

Por este motivo, el sentido de este análisis ha sido realizar una aproximación a los aspectos más destacados de la transferencia internacional de datos, teniendo en cuenta que la dificultad en la protección de estos datos que se transfieren a otros países radica en la adaptación de la LOPD a aquellos países que no presenten nivel de protección equivalente al del país de origen de ese ciudadano demandante de empleo[30]. Por tanto, se ha intentado delimitar su ámbito de actuación teniendo en cuenta que esos datos, al ser

[29] En este supuesto es obligatorio interponer la denominada política de privacidad o aviso legal, siguiendo lo establecido en el art.10 de la Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE núm.166 de 12 de julio de 2002) que describe el contenido mínimo que debe tener las condiciones de uso de la web y en lo que lo que respecta a la protección de datos de carácter personal se deben seguir las siguientes pautas: "*Protección de datos. Para la obtención de datos personales, información a los interesados y creación y mantenimiento de ficheros de datos personales, será de aplicación la LOPD. En el caso en que desde la página web se recojan datos de carácter personal a través de formularios de recogida de datos se habrá de incluir en el aviso legal el principio de información regulado en el artículo 5 de la LOPD, estableciendo una política o aviso de privacidad que recoja los siguientes extremos: Existencia de un fichero al que serán incorporados los datos que se solicitan. Identidad y dirección del responsable del fichero/tratamiento. Finalidad para la que serán usados los datos, La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación u oposición al tratamiento de los datos. Igualmente, si son utilizados otros mecanismos de seguimiento de la navegación de usuario y obtención de determinados datos (archivos comúnmente denominados cookies), existe la obligación de informar al usuario de su utilización, finalidades, así como de los mecanismos para poder desactivar estos archivos de sus sistema/ordenador."*

[30] Sobre el concepto de transferencia internacional de datos: TRONCOSO REIGADO, A.: *Comentario a la Ley Orgánica de protección de datos de carácter personal*, Thomson-Reuters, 2010.pp.1775-1784.LESMES SERRANO, C. (coord.): *La Ley de Protección de Datos: análisis y comentario de su jurisprudencia,* Lex Nova, 2008.pp.553-557.

transmitido por medios tecnológicos, quedan almacenados en los servidores webs. Asimismo, se ha considerado importante conocer si en la política de privacidad de las agencias de intermediación y de los demás mecanismos que propician el acceso al empleo, ya citados, se contempla la posibilidad de comunicar los datos a otros países y si esa cesión e ajusta a la legalidad.

El tercer bloque de este trabajo se ha dedicado a examinar la aplicación del derecho a la protección de datos de los trabajadores en el marco empresarial, es decir, una vez que el ciudadano ha conseguido un empleo. Haciendo referencia a la premisa dada por el Tribunal Constitucional[31], en la que se expone que: *"La celebración de un contrato de trabajo no implica en modo alguno la privación para una de las partes, el trabajador, de los derechos que la Constitución le reconoce como ciudadano*", se ha pretendido dar importancia a los derechos fundamentales, entre los que se encuentra el derecho a la protección de datos de carácter personal dentro de la relación de trabajo para que puedan ser ejercidos y respetados en la empresa, aunque el trabajador esté sometido al ámbito de supervisión y organización del empresario.

La problemática que se ha tratado en el tercer capítulo ha exigido marcar el siguiente esquema de trabajo: en primer lugar, se han enumerado todos aquellos datos que necesita conocer el empresario para poder administrar el desarrollo de una relación de trabajo. En este sentido, no sólo se hace necesario conocer datos generales, sino que, en ocasiones, tendrá que conocer algunas informaciones consideradas como especialmente sensibles por la normativa sobre protección de datos -salud y afiliación sindical[32]- para

[31] Sentencia del Tribunal Constitucional de 12 de junio de 1996 (RTC 1996, 106).
[32] Art. 7.2 y 7.3 de la LOPD: *"2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. 3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente."*

realizar una correcta gestión de personal. Pero para ello no es suficiente el simple acceso a esas informaciones, sino que tiene que registrarla y almacenarla en ficheros lo que constituye, como es sabido, un tratamiento de datos de carácter personal sometido a los principios establecidos en la LOPD. Todos estos aspectos controvertidos relativos a la contratación del trabajador y a la organización de las relaciones de trabajo, se han ido exponiendo a lo largo de este capítulo estableciendo que procesamiento de datos son legítimos y cuáles no cumplen con las prerrogativas establecidas en la legislación sobre protección de datos de carácter personal.

En segundo lugar, se ha procedido a identificar los distintos responsables de ficheros que tienen cabida cuando lo que se pretende es utilizar los datos de los trabajadores para la correcta administración del personal de la empresa, identificación imprescindible para poder para poder exigir las obligaciones relacionadas con el cumplimiento de los principios de la LOPD. Y en tercer lugar, se ha considerado preciso especificar los requisitos que deben tener esas bases de datos y las medidas de seguridad que se tienen que implantar destinadas a proteger la información de los trabajadores allí contenidos, así como las comunicaciones de datos que el empresario tenga que realizar para llevar a cabo una correcta gestión del personal de su empresa, puntualizando aquellas cesiones de información efectuados a los representantes unitarios de los trabajadores y a los sindicatos.

Por último en el cuarto y último capítulo de la presente investigación se ha realizado un análisis de las vicisitudes que pueden tener lugar en el centro de trabajo y que pueden afectar al derecho a la protección de datos de los trabajadores. Lógicamente, la mayor amenaza para este derecho fundamental de los trabajadores la presentan las TICS, pues la propia naturaleza de estos mecanismos hace que se lleguen a informatizar muchos datos personales de los trabajadores analizados desde una doble vertiente; por un lado, desde el apoyo en la gestión organizativa de la empresa que proporcionan herramientas como la intranet o los teléfonos de empresa; y de otra parte, como instrumentos que faciliten al empresario las labores de supervisión de la relación de trabajo

(control de acceso a través de medios electrónicos, email, navegación por internet).

Se ha tratado pues de hacer una descripción somera sobre cómo esos medios pueden llegar a tratar datos de carácter personal y el grado de cumplimiento de la LOPD en los diferentes supuestos presentados, relacionados con la organización y control de los trabajadores. Es cierto, que esta problemática ha sido abordada por distintos autores, muchos citados a lo largo de esta trabajo de investigación pero lo que se ha intentado, con la inclusión de este apartado, es dar un punto de vista más restringido, pretendiendo desligar estos aspectos del derecho a la intimidad para que haya una visión más amplia de lo que interfieren determinadas actuaciones en el derecho a la protección de datos de los trabajadores.

El último eslabón de este cuarto capítulo lo ha conformado el análisis del destino de esos datos cuando la relación de trabajo se ha extinguido por alguno de los motivos establecidos en el art. 49.1 del Estatuto de los Trabajadores[33] .Pues, no tiene sentido que el empresario mantenga la información de aquellos trabajadores que no pertenecen a su centro de trabajo, por este motivo se hace preciso observar el nivel de cumplimiento del derecho de cancelación de aquellos trabajadores que ya no pertenezcan al ámbito organizativo empresarial y en qué casos es posible el mantenimiento de esas bases de datos y bajo qué garantías.

La estructura de la investigación ha puesto de manifiesto la exclusión de todos aquellos problemas que puedan plantearse en el centro de trabajo que no requieran la realización de un tratamiento de datos de carácter personal. La extensión del tema, su aplicación a los supuestos basados en la búsqueda de empleo y en el desarrollo de la actividad laboral, así como la cantidad de cuestiones y problemas concretos que se plantean desaconsejan un estudio global relativo al simple acceso a los datos sin que medie cualquier actuación de las definidas en el en el art. 3 c) de la LOPD. Si así se hiciera esta

[33] RD 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (BOE de 29 de Marzo de 1995).

investigación podría recaer en la realización de un examen parcial e incompleto, ante la amplitud de cuestiones que podrían darse relacionadas con el acceso y visualización de la información de carácter personal de los sujetos sometidos a este estudio. Sin embargo, en los capítulos desarrollados se pretende hacer una distinción entre acceso y tratamiento de datos para, así, poder profundizar en la problemática relativa al procesamiento y cesión de datos.

Tampoco se ha estimado efectuar un estudio amplio de la legislación existente en los distintos países europeos sobre la custodia de los datos de carácter personal, pues esta temática podría dar lugar a un trabajo de investigación basado íntegramente en la comparación de normativas. Pero sí se ha procurado examinar estas normas haciendo ciertas distinciones y citando algunos países que sí disponen de una norma específica sobre la protección de datos del trabajador lo que podría orientar posibles mejoras en el tratamiento de los datos personales de los empleados trabajador en nuestro país, configurando una normativa protectora de la información de carácter personal en el ámbito laboral.

Otro de los aspectos que no han sido abordados de forma concreta es el tratamiento de datos que realiza la propia empresa cuando ella misma instrumenta un proceso de selección de personal, sin que medie ninguna otra entidad intermediaria. En este sentido, se va a observar como la propia lógica de la elección del candidato más idóneo, para un determinado puesto de trabajo, discurre de igual forma si lo hace la propia empresa o cualquier otro centro de intermediación laboral. Lo mismo ocurre con el tratamiento de datos, el cual tiene las mismas exigencias para una empresa u otra, quizás con algunas distinciones relativas a la comunicación de datos a terceros, las cuales se producen una vez que el trabajador es contratado[34].

[34] Estas comunicaciones pueden basarse en las que se efectúan a la gestoría externa para la realización de las gestiones relativas a la contratación del trabajador o aquellas que tienen que ver con la vigilancia de la salud de los mismos gestionada por una empresa de prevención de riesgos. Aunque, en ocasiones, se puede prescindir de estas cesiones si es la propia empresa para que realiza esos trámites, los cuales no tienen nada que ver con acceso al empleo, pues tienen lugar una vez que el trabajador ha sido seleccionado y va a entrar a formar parte de la empresa.

En definitiva, el resultado de la investigación realizada es fundamentalmente práctica y adaptada a la realidad de la gestión de datos del personal en la empresa y es, en este sentido, dónde se ha intentado incidir y dar soluciones a los posibles conflictos que puedan surgir en el tratamiento de la información personal de estos trabajadores.

CAPITULO I: CONFIGURACIÓN DEL SISTEMA DE PROTECCION DE DATOS DE CARÁCTER PERSONAL Y SU PROYECCIÓN EN EL ÁMBITO DE LAS RELACIONES LABORALES

Sumario: 1. CUADRO NORMATIVO SOBRE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL. 1.1. Breve referencia al marco europeo sobre protección de datos de carácter personal. 1.2. Regulación y contenido del derecho a la protección de datos de carácter personal en España. **2. LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL COMO DERECHO FUNDAMENTAL Y AUTÓNOMO.** 2.1. El derecho a la protección de datos como derecho fundamental inespecífico. **3. EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LAS RELACIONES DE TRABAJO. 3**.1. Ámbito de aplicación de la normativa sobre protección de datos y su afectación a las relaciones laborales. 3.2. Configuración del concepto de dato de carácter personal. 3.3. Los principios de la protección de datos de carácter personal. 3.3.1. Principio de calidad. 3.3.2. Principio de información. 3.3.3. Principio de consentimiento. 3.4. Derechos relativos a la protección de datos de carácter personal. **4. OBLIGACIONES IMPUESTAS A LOS SUJETOS ENCARGADOS DE LOS FICHEROS DE DATOS.** 4.1. Breve referencia a los sujetos encargados de la protección de datos. 4.2. Significado y alcance de los ficheros de datos de carácter personal. 4.3. Establecimiento de medidas de seguridad en los ficheros de datos de carácter personal. **5. INSTITUCIONES DE CONTROL DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.** 5.1. La Agencia Española de Protección de Datos. 5.2 Descentralización de la protección de datos de carácter personal: las agencias autonómicas de control de la protección de datos de carácter personal.

CAPITULO I: CONFIGURACIÓN DEL SISTEMA DE PROTECCION DE DATOS DE CARÁCTER PERSONAL Y SU PROYECCIÓN EN EL ÁMBITO DE LAS RELACIONES LABORALES.

La protección de datos de carácter personal implica el surgimiento de uno de los derechos denominados de tercera generación[35], derechos que adquieren cada vez un mayor protagonismo conforme se van produciendo avances y desarrollos significativos de las tecnologías de la información y la comunicación. En efecto, son estos avances los que han provocado que, poco a poco, se vaya dando forma y contenido al derecho a la protección de datos como respuesta a las posibles vulneraciones que, respecto de derechos fundamentales tradicionales como el de intimidad, se pueden producir mediante el tratamiento informatizado de los datos de carácter personal. Reflejo de ello son reformas normativas que se han ido sucediendo a partir de lo establecido en el art. 18.4 de la Constitución Española[36].

A estos efectos y siguiendo el mandato constitucional, la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen[37], contempló en su disposición transitoria primera[38] la salvaguarda de los datos de carácter personal mientras

[35] RUIZ MIGUEL, C.: "La tercera generación de los derechos fundamentales" *Revista de estudios políticos*, núm.72, 1991, pág. 303; PÉREZ LUÑO, A.E.: *"*Libertad Informática. Nueva frontera de los derechos fundamentales*",* en el vol. de LOSANO*,* M., *La libertad informática y leyes de protección de datos personales,* Centro de Estudios Constitucionales, Madrid, 1989, pp. 137-162; VIDAL GIL. E.: "Los derechos de tercera generación" en MEGÍAS QUIRÓS, J.J.(coord.): *Manual de derechos humanos: los derechos humanos en el siglo XXI*, Aranzadi, 2006, pp.121-135; PÉREZ LUÑO, A.E.: *La tercera generación de los derechos humanos*, Aranzadi, 2006, pp.31-32; MORAES REGO, N.: *La contribución del poder judicial a la protección de los derechos humanos de la tercera generación*, Ediciones Salamanca, 2014, pp. 72-73; HERRÁN ORTIZ, A.I.: *La violación de la intimidad en la protección de datos personales*, Dykinson, 1999, pág. 72.

[36] Sobre la repercusión del art. 18.4 CE en la configuración del derecho a la protección de datos: PÉREZ LUÑO, A.E.: "Informática y libertad. comentario al art. 18.4 de la constitución española", *Revista de Estudios Políticos*, núm. 24, 1981, pp. 46 y ss.; MURILLO DE LA CUEVA, P.L.: *El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática"*, Tecnos, 1991, pp. 150-158; ROIG I BATALLA, A.: "La protección de la privacidad: el derecho al honor y la intimidad personal y familiar, y los límites al uso de la informática(arts. 18.1 y 18.4 CE)"en VV.AA.: *Constitución: desarrollo, rasgos de identidad y valoración en el XXV aniversario (1978-2003)*, 2004, pp. 107-120.

[37] BOE núm.115 de 14 de mayo de 1982.

[38] Disp. Transitoria 1ª*: "En tanto no se promulgue la normativa prevista en el art. dieciocho, apartado cuatro, de la Constitución, la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley".*

no se promulgara una norma específica que regulara dicha protección. Es llamativo, no obstante, que en esta norma, ya posterior al texto constitucional, no se hiciera alusión de forma expresa a lo contenido en el art. 18.4 de la CE[39]; aunque este hecho puede tener su justificación en el propósito de que su regulación se hiciera a través de una ley global que perfilara, de forma sistemática, los distintos aspectos de la tecnologías informáticas que podrían afectar al ejercicio del derecho a la protección de datos de carácter personal.

Este propósito se materializó, años más tarde, en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal[40]. Se trata de una norma que, afrontando la carencia de una disciplina jurídica integral de la protección de datos de carácter personal, se decantó por su necesidad y conveniencia. No obstante, las dudas

[39] Hay Estados europeos en los que se ha reconocido expresamente este derecho en sus Constituciones. Es el caso del Instrumento de Gobierno sueco (La constitución sueca está compuesta de cuatro leyes, y la que hace alusión a la protección de datos de carácter personal es la de Instrumento de Gobierno de 1974, disponible en *http://www.wipo.int/wipolex/es/*); "*Ningún dato sobre un ciudadano recogido en registros públicos podrá basarse sin su consentimiento, exclusivamente en sus opiniones políticas. Se protegerá a los ciudadanos en la medida precisada por la ley contra cualquier lesión de su integridad personal resultante del almacenamiento de datos que les afecten, mediante tratamiento informático"; también* del art. 35 de la Constitución Portuguesa de 1976 (Diario de la República Portuguesa, 25 de abril de 1976 disponible en: *https://dre.pt/constituicao-da-republica-portuguesa*), la cual tuvo bastante influencia en nuestra Constitución, pues fue la precursora de que se incluyera el término informática en la misma; "*Todos los ciudadanos tienen el derecho de acceso a los datos informatizados relativos a ellos y puede requerir su corrección y actualización, y el derecho a conocer el destino, conforme a la ley. 2. La ley define los datos personales, así como las condiciones aplicables al tratamiento automatizado, conexión, transmisión y utilización, y garantiza su protección, incluso a través de un órgano administrativo independiente. 3. El equipo no puede ser utilizado para el tratamiento de los datos de las convicciones filosóficas o políticas, partidos o sindicatos, las creencias religiosas, la privacidad y el origen étnico, excepto por autorización expresa, la autorización prevista por la ley con garantías de no discriminación o para procesamiento los datos estadísticos no identificar a los individuos. 4. Está prohibido acceder a los datos personales de terceros, salvo en los casos excepcionales previstos por la ley. 5. La ley prohíbe la asignación de un número nacional único para los ciudadanos. 6. Se garantiza a todos el libre acceso a las redes de ordenadores para uso público, la ley que define las normas aplicables a los flujos transfronterizos de datos y las formas apropiadas de protección de datos personales y otras medidas preventivas que estén justificadas por razones de interés nacional. 7. Los datos personales guardados en los archivos manuales se beneficiarán de una protección idéntica a la prevista en los párrafos precedentes, conforme a la ley".* Finalmente, en otros Estados europeos, el derecho a la protección de datos de carácter personal no se menciona de forma directa, aunque existan disposiciones que puedan relacionarse con el sistema seguido en España (art. 18.4 CE), como es el caso del art. 2 de la Constitución Italiana (Constituzione della Repubblica Italiana, de 22 de diciembre de 1947, *Gazzetta Ufficiale* del 27 diciembre de 1947, n.298): "*La República reconoce y garantiza los derechos inviolables del hombre, como individuo y en los grupos sociales en la personalidad humana, y requiere el cumplimiento de los deberes imperativos de la solidaridad política, desarrollo económico y social*".

[40] BOE núm. 262 de 31 de octubre de 1992.

acerca de su pertinencia no se habían despejado entre los juristas[41]. De hecho, algunos autores[42] han establecido un interesante debate sobre los términos adecuación y pertinencia de los datos pero, en materia laboral, estos conceptos deben atender, por un lado, a la cantidad de datos necesarios para lograr la finalidad pretendida por el empresario, en este caso, cumplimentar el contrato de trabajo y, por otro, a la exigencia de no pedir y tratar más información de la necesaria para identificar a cada trabajador, en los términos amplios antes dichos.

A pesar de las deficiencias de la LORTAD, en su exposición de motivos aparece por primera vez una referencia a la protección de datos relacionada

[41] MURILLO DE LA CUEVA, P.L.: "La construcción del derecho a la autodeterminación informativa", *Revista de Estudios Políticos*, núm.104, 1999, pp. 35-37. Si se analiza el panorama europeo, se observa como otros ordenamientos han previsto algunas legislaciones específicas que sí tratan el derecho a la protección de datos de carácter personal. Así, la Lei 7/2009, de 12 de febrero, que aprueba la revisión del Código de Trabajo portugués (Diario de la República Portuguesa 1ª serie- Nº30-12 de febrero de 2009) muestra en su articulado (arts. 17-22) algunas referencias a la protección de datos de los trabajadores relativas a los derechos de la personalidad en el lugar de trabajo, uso de los datos biométricos, mecanismos de video vigilancia y sobre informaciones médicas de los trabajadores. En el derecho italiano se puede acudir a lo establecido en los arts. 4, 6 y 8 del Statuto dei Lavoratori (Legge núm. 300, de 20 de mayo de 1970, Statuto dei Lavoratori publicada en la Gazeta Ufficiale, de 27 de mayo de 1970), en los que se hace alusión, al igual que en los arts. 18 y 20 del ET, a la instalación de medios audiovisuales de control, prohibiendo su uso, y sólo admitiéndolo, cuando sea necesario para una correcta organización productiva y para implantar medidas de seguridad en el centro de trabajo. También se hace mención a las "visitas" para controlar a los trabajadores, permitiéndolas tan solo si son imprescindibles para proteger el patrimonio empresarial y a la prohibición por parte del empresario de hacer indagaciones sobre aspectos ideológicos del trabajador. En el Código de Trabajo francés (Article 1221-6 Code du Travail, aprobado por Loi nº 99/2003, de 27 de agosto (http://www.legifrance.gouv.fr) también se establece que las informaciones solicitadas a los candidatos a un empleo sólo podrán tener como objetivo valorar su capacidad para ocupar el empleo ofertado. Sobre estos aspectos vid. COELHO MOREIRA, T.:*A privacidade dos trabalhadores e as Novas Tecnologías de Informacao e Comunicacao: contributo para um estudo dos limites do poder de controlo electrónico do empregador,* Almedida, 2010; RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, M.: "Del Statuto dei lavoratori al Estatuto de los trabajadores. Dos experiencias en contraste" en VV.AA.: *El Estatuto de los Trabajadores Italiano veinte años después*, Ministerio de Trabajo y Seguridad Social, 1993, pág.151; RAY J.E.: "Une loi macédonienne? Etude critique du titre V de la Loi du 31 décembre 1992: Dispositions relatives au recrutement et aux libertés individuelles", *Revista Droit Social*, núm. 2, 1993, pp. 103-114; MOLE, A.: "Au delá de la informátique et libertés", *Revista Droit Social*, núm.6, 1992, pp. 603-605.

[42] Así MURILLO DE LA CUEVA, P.L. mantiene que adecuaciòn son tèrminos sinònimos pero con matices que hacen referencia a la idoneidad de los datos respecto a la finalidad del fichero de datos, en MURILLO DE LA CUEVA, P.L.: *Informatica y...*op. cit., pág. 65; HERRÁN ORTIZ establece que la adecuaciòn hace referencia a la conexiòn del dato con la finalidad mientras que la pertinencia con la necesidad de no solicitar màs datos de los necesarios para cumplir el objetivo, en HERRÁN ORTIZ, A.I.: *La violación de la intimidad en la protecciòn de datos personales*, Dykinson, 1999, pág. 243; SERRANO PÉREZ, establece que los conceptos adecuaciòn y pertinencia no se solapan, sino que establecen matices diferentes para aludir a la cantidad y calidad de los datos, en SERRANO PÉREZ, M.:*El derecho fundamental a la protecciòn de datos*, Civitas, 2003, pp. 437-443.

con el ámbito laboral, al señalar que: "*Aún más: el conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor; y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos".*

Con la intención de adaptar la normativa nacional a los criterios impuestos por la normativa comunitaria, materializados en la Directiva 95/46/CE, se aprueba la actual Ley 15/1999, de 13 de diciembre, sobre protección de datos de carácter personal[43], en torno a la cual se van a tratar a lo largo de este capítulo algunos aspectos definitorios y de contenido para, más tarde, poder proyectarlos a la casuística relacionada, tanto con el acceso al empleo y el desarrollo de la relación de trabajo, como con las vicisitudes generadas en conexión con este derecho a la hora de extinguir la relación de trabajo. Cierto es que estos aspectos son de carácter general, pues no se puede hablar de que esta norma sea específica de trabajadores, ya que en ningún precepto de la norma se hace alusión a los mismos, aunque esté prevista alguna particularidad en cuanto a las excepciones que presenta el principio del consentimiento, como se analizará cuando llegue el momento de abordarlo.

Para terminar de hacer la enumeración inicial de las normas relativas a la protección de datos, hay que hacer referencia al Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, el cual viene a cumplir con el mandato dispuesto en la disposición final primera de la LOPD[44]. Es obvio que esta normativa de desarrollo del derecho a la protección de datos pretende, por un lado, aportar cierta claridad y seguridad jurídica al sistema, perfilando conceptos y aportando una guía que permita el

[43] BOE núm. 298 de 14 de diciembre de 1999.
[44] En este sentido, la Disp. Fin. 1ª de la LOPD establece que: "*El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley".*

cumplimiento de la normativa de protección de datos y, por otra parte, dotar al sistema normativo de una cierta flexibilidad que permita una aplicación eficaz por parte del responsable del fichero[45].

1. CUADRO NORMATIVO SOBRE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

1.1. Breve referencia al marco europeo sobre la protección de datos de carácter personal.

El derecho a la protección de datos en Europa tuvo su origen en la actividad del Tribunal de Justicia de la Comunidad Europea[46], pues previamente a la aprobación de un texto normativo sobre protección de datos en el ámbito europeo, el TJCE ya había resuelto algunos casos que atentaban contra este derecho.

El primer caso relativo a la protección de datos resuelto por el TJCE es el conocido como caso Stauder[47], que puede considerarse una Sentencia pionera sobre la protección de datos de carácter personal y a la que siguieron otras relacionadas, en las que el TJCE ha resuelto unas veces a favor de la existencia de la citada protección[48], y otras sin tenerla en cuenta[49].

---

[45] MARTÍNEZ MARTÍNEZ, R.: "El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Aspectos claves", *Revista jurídica de Castilla y León*. núm. 16, 2008, pp. 264-266.

[46] Contrariamente, algunos autores mantienen que este derecho, a diferencia de lo que ha sucedido con otros, se ha introducido vía legislación y posteriormente se ha desarrollado por la jurisprudencia. Se apoyan en el hecho de que el TJCE sí había reconocido el derecho a la vida privada, pero no un derecho a la protección de datos personales. Vid. RUIZ MIGUEL, C.: "El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea", en *Revista de Derecho Comunitario Europeo*, núm. 14, 2003, pág. 15.

[47] Sentencia del TJCE de 12 de noviembre de 1969 (Asunto C-29/69): Caso de un ciudadano alemán al que se le entrega un cupón para comprar mantequilla a precio reducido en virtud de una Decisión de la Comisión. Los cupones eran nominativos, para que se beneficiaran de esta ayuda las personas que tuvieran derecho a ella por sus circunstancias económicas. El ciudadano considera que revelar su nombre y su condición económica era contrario a su dignidad personal, aunque el TJCE no hace ninguna referencia en su resolución a un derecho a la protección de datos pero si entendemos que el nombre es un dato personal (como ha hecho el Tribunal Europeo de Derechos Humanos), estaríamos ante un caso de protección de datos dónde se produce una cesión de los mismos a los vendedores.

[48] Así sucede en el caso Internationale Handelsgesellschaft (STJCE de 17 de diciembre de 1970, Asunto C-11/70) y, de forma más clara, en el caso Nold (STJCE de 14 de mayo de1974, Asunto C-4/73), donde se afirma ya la protección del derecho a la protección de datos como

Como consecuencia de las diversas resoluciones jurisprudenciales y de la intención de unificar criterios debido a que en cada Estado Miembro se regulaba esta materia de una forma distinta, se suscribió el Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[50], con la finalidad de atender a la necesidad de una regulación del derecho a la protección de datos. El objetivo más inmediato de este Convenio era garantizar en todo el territorio de la Unión Europea el respeto al derecho a la vida privada en relación con el tratamiento automatizado de los datos personales de cada individuo. A pesar de estos anhelos unificadores, esta propuesta europea no tuvo la aceptación esperada por lo que posteriormente se aprobaron varias directivas comunitarias que regulaban la protección de datos de carácter personal[51.]

---

parte integrante del Derecho comunitario con expresa referencia a las tradiciones constitucionales comunes y a los tratados internacionales sobre derechos fundamentales. Vid. BALAGUER CALLEJÓN, F.: "Derecho y derechos en la Unión Europea", en CORCUERA ATIENZA, J. (coord.), *La protección de los derechos fundamentales en la Unión Europea*, Dykinson, 2002, pág. 44 y RODRÍGUEZ BEREIJO, A.: "La Carta de los derechos fundamentales de la Unión Europea y la protección de los derechos humanos" en FERNÁNDEZ SOLA, N. (coord.): *Unión Europea y Derechos fundamentales en perspectiva constitucional,* Dykinson,, 2004, pp. 11-13. Críticos con esta postura, RUBIO LLORENTE, F.: "Mostrar los derechos sin destruir la Unión", Revista Española de Derecho Constitucional, núm. 64, 2002, pp. 15-18.

[49] Así sucede con la STJCE, de 7 de octubre de 1987, caso Strack: *"…Considera que debería ser posible acceder, a través de la consulta de este expediente, a las actas de los exámenes médicos regulares del Sr. Strack, los datos recogidos acerca del accidente de trabajo de 1970 y los diagnósticos de los médicos y peritos designados por la Comisión, dado que dichos documentos están intrínsecamente vinculados a las funciones desempeñadas por el funcionario…Respecto a la calificación de los documentos cuyo acceso solicita la demandante a través de la consulta del expediente personal, hay que señalar que los informes realizados por los médicos y peritos revisten sin duda un carácter exclusivamente médico. Los documentos relativos a los datos recogidos acerca de un incidente producido durante el trabajo, que pueden servir de fundamento a un procedimiento para que se reconozca la existencia de un accidente de trabajo o de una enfermedad profesional en el sentido de la Reglamentación, deben considerarse también de carácter médico, lo cual no impide que dichos documentos puedan, en su caso, afectar también a la situación administrativa del funcionario, por haberse utilizado los hechos que relatan como base para informes sobre su competencia, rendimiento o comportamiento. En tal caso, dichos documentos deben figurar en el expediente personal…. En tales circunstancias, procede declarar que la Comisión permitió el acceso de la demandante al expediente personal completo de su difunto marido y que estaba legitimada para denegarle el acceso a los documentos de carácter médico fuera del procedimiento especial previsto a tal efecto".*

[50] Ratificado por España y publicado en BOE núm. 274, de 15 de noviembre de 1985.

[51] TÉLLEZ AGUILERA, A.: *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*, Edisofer, Madrid, 2002, pp. 26-58; MOLDOF, S.: "International Employee Privacy: union/employ y perspective" en REMY NASH, J.: *Workplace Privacy*,KluwerLaw International, 2010, pp.140-146.

La primera de ellas, la Directiva 95/46/CE[52], nació para aunar criterios en lo que a la protección de datos de carácter personal se refiere, con la finalidad de favorecer el mantenimiento de relaciones comerciales y personales con otros países[53]. A este fin, contiene la definición de datos personales, el reconocimiento de los derechos de los titulares de datos personales (derecho a ser informado, derecho a la libre disposición de los datos, y derechos de acceso, rectificación y cancelación), los principios que deben regir cualquier tratamiento de datos que se lleve a cabo, previendo también la limitación de dichos derechos y principios en determinados casos.[54]

La Directiva 95/46/CE ha sufrido muchas modificaciones de adaptación sobre todo en lo relativo a las comunicaciones electrónicas. Por esta razón, se aprobó la Directiva Europea 97/66/CE, de 15 de diciembre de 1997, relativa al tratamiento de datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones[55], que tradujo los principios enumerados en la Directiva 95/46/CE en normas concretas para el sector de las telecomunicaciones, siendo sustituida por la Directiva 2002/58/CE, de 12 de

[52] La Directiva 95/46/CE, además de en España, tuvo acogida en otros países europeos a través de la adecuación de la normativa existente a los criterios implantados por la norma comunitaria, como es el caso de Francia con la Loi nº78-17 du 6 janvier 1978 relative á l'informatique, aux fichiers et aux libertés (Journal officiel du 7 janvier 1978) que finalmente no fue sustituida, sino que se fue adaptando a los cambios sin necesidad de promulgar una nueva norma. En contraposición, en Portugal se aprobó Lei núm. 67/98, de 26 de outubro, de datos personales (Diario de la República portuguesa serie-A Nº 247 de 26 de outubro de 1998) y en Suecia la Ley 1998/204 de Datos Personales de 29 de abril de 1998 (Personuppgiftslagen 1998:204 of 29 April o Personal Data Act), debido a la inexistencia de una norma que tratara la protección de datos de carácter personal. Sobre estas trasposiciones al derecho interno, véase: BRU CUADRADA, E.: "La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad", *Revista de Internet, Derecho y Política*, núm. 5, 2007, pp.79-80; ARENAS RAMIRO, M; *El derecho fundamental a la protección de datos personales en Europa,* Dykinson, 2006*,* pp. 421-423; ABJORSSON, B.: "Relación entre la protección de datos y la libertad de prensa y de expresión" en TRONCOSO REIGADA, A, (dir): *Transparencia administrativa y protección de datos personales*, Civitas, 2008, pp. 304-305.

[53] Vid., http://europa.eu/scadplus/constitution/objectives_es.htm#PRINCIPLES

[54] Sobre la Directiva 95/46/CE véase: MARTIN-CASALLO LÓPEZ, J.J.: "Implicaciones de la Directiva sobre protección de datos en la normativa española", *Actualidad Informática Aranzadi,* núm.20, 1996, pp. 1 y ss.; BETÉS DE TORO, A.: "El derecho de información y los principios legitimadores del tratamiento automatizado de los datos de carácter personal en la Directiva 95/46/CE, de 24 de octubre de 1995", *Actualidad Informática Aranzadi,* núm. 25, 1997, pp. 6 y ss.; DAVARA RODRÍGUEZ, M.A.A.: *La protección de datos en Europa*, *principios, derechos y procedimiento,* Universidad Pontificia de Comillas, 1998, pp. 41 y ss.; GARCÍA-BERRIO HERNÁNDEZ, T.: *Informática y libertades: La protección de datos personales y su regulación en España y Francia,* Servicio de publicaciones de la Universidad de Murcia, 2003, pp. 109-114.

[55] DOCE núm. L 024 de 30, de enero de 1998.

julio, relativa al Tratamiento de Datos Personales y Protección de la Intimidad en el sector de las Comunicaciones Electrónicas[56], incrementando el compromiso de los Estados Miembros de armonizar las legislaciones nacionales relativas al tratamiento de datos de carácter personal[57] para dar respuesta a las vulneraciones del derecho a la protección de datos que se producen por el envío de informaciones a través de los medios informáticos. Algo de gran relevancia, por cierto, en el ámbito laboral ya que, como se sabe, el empresario suele agilizar los trámites administrativos, relacionados con la política de personal, utilizando las tecnologías más avanzadas de comunicación[58].

Es en el año 1997, con las reformas introducidas por el Tratado de Ámsterdam[59], cuando el derecho a la protección de datos de carácter personal entra a formar parte de la normativa europea originaria o fundamental. Así, en el art. 286 del Tratado se establece que: *"A partir del 1 de enero de 1999, los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos establecidos por el presente Tratado o sobre la base del mismo. 2. Con anterioridad a la fecha indicada en el apartado 1, el Consejo establecerá, con arreglo al procedimiento previsto en el art. 251, un organismo de vigilancia independiente, responsable de controlar la aplicación de dichos actos comunitarios a las instituciones y organismos de la Comunidad y adoptará, en su caso, cualesquiera otras disposiciones pertinentes."* Como desarrollo del mandato contenido en este art., se aprobó el Reglamento 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los

[56] DOCE núm. L 201, de 31 de julio de 2002.
[57] GARCÍA-BERRIO HERNÁNDEZ, T.: *Informática y libertades: La protección…,* op. cit., pp. 107-108.
[58] MENÉNDEZ SEBASTIÁN, P.: "Protección de datos personales del trabajador (Directiva 95/46/CE)" en VV.AA: *La transposición del Derecho Social Comunitario al ordenamiento español,* Ministerio de Trabajo y Asuntos Sociales, 2005, pp. 411-413; ARENAS RAMIRO, M.: "La protección de datos personales en los países de la Unión Europea", Revista Jurídica de Castilla y León, núm.16, 2008, pp.123-124.
[59] DOCE núm. C 340, de 10 de noviembre de 1997.

organismos de la Comunidad y sobre la libre circulación de estos datos[60], Reglamento actualmente en vigor y que ha dado origen a la figura del "Supervisor Europeo de Protección de Datos", entidad independiente cuya función es garantizar que las instituciones y organismos de la UE respeten el derecho de las personas a la intimidad en el tratamiento de sus datos personales, no sólo colaborando con los responsables de la protección de datos de cada institución u organismo, sino también velando porque se apliquen las normas de confidencialidad de dichas informaciones[61].

En el mismo año 2000 se proclama en Niza la Carta de los Derechos Fundamentales de la Unión Europea, reconociendo en su art. 8[62] el derecho a la protección de datos personales. La Carta de DDFF[63], aunque no permite que los derechos en ella reconocidos tengan la fuerza normativa de los derechos fundamentales, sirve para separar el derecho a la protección de datos del derecho a la vida privada consagrado en el art. 8 del Convenio para la protección de los derechos humanos y de las libertades fundamentales[64]. A estos efectos, la afirmación del derecho a la protección de datos como derecho fundamental ha sido solventada, en primer lugar, con la Constitución Europea[65], que lo incluye como parte de su articulado (en su art. II-68,

[60] DOCE núm. L 008, de 12 de enero de 2001.
[61] SCIROCCO, A.: "Acceso a documentos y protección de datos personales: la experiencia del Supervisor Europeo de Datos Personales" en TRONCOSO REIGADA, A, (dir).: *Transparencia administrativa y*…, op. cit., pág. 296; PAGALLO, U.: *La tutela della privacy negli stati unitid'America e in Europa*, Giuffre Editore, 2008, pp. 109-116.
[62] Art. 8 de la Carta de Derechos Fundamentales de la UE (DOCE núm. C 364/1 de 18 de diciembre de 2000): "*1.Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".*
[63] Para un conocimiento exhaustivo acerca de la evolución en la protección de los Derechos humanos en la Unión Europea resulta fundamental: DE LA VILLA GIL, L.E.: "La Carta de los Derechos fundamentales de la Unión europea", *Revista del Ministerio de Trabajo y Asuntos Sociales*, núm. 32, 2001, pp. 13-18; PEREZ DE LOS COBOS, F.: *El derecho social comunitario en el Tratado de la Unión Europea*, Madrid, Civitas, 1994, pág. 24.
[64] Art. 8 del Convenio Europeo de Derechos Humanos (BOE núm. 108 de 6 de mayo de 1999): "*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones".*
[65] Tratado de Roma, firmado en Roma, el 29 de octubre de 2004, con entrada en vigor el 1 de noviembre de 2006 (DOUE núm. C 310, 16 de diciembre de 2004).

reproduciendo el art. 8 de la Carta; y en su art. I-51, reproduciendo el art. 286 del TCE)[66]; y, en segundo lugar, con el art.6[67] del Tratado de Lisboa.

Además de las disposiciones y Directivas citadas, se han instaurado otros instrumentos comunitarios que permiten abordar la aplicación del derecho a la protección de datos de carácter personal en el ámbito laboral ya que en la Directiva 95/46/CE únicamente se hace una referencia específica a las relaciones laborales en el art. 8, apartado 2, relativo al tratamiento de datos sensibles. Desde esta perspectiva, se han hecho algunas Recomendaciones[68], destacando la del Consejo de Europa, sobre la protección de datos de carácter personal utilizados con fines de empleo[69], referida a las relaciones entre empresario y trabajador, que contiene una serie de consideraciones generales sobre las posibilidades de tratar legítimamente los datos de los trabajadores.[70]

---

[66] Art. II-68: "*1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente.* Art. I-51: "*1.Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. La ley o ley marco europea establecerá las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes".*

[67] Vid., art. 6 Tratado de Lisboa (DOUE núm. C 306, de 17 de diciembre de 2007).

[68] DAVARA RODRÍGUEZ, M.A.: *La protección de datos*…, op. cit., pp. 29-47.; ARENAS RAMIRO M.: *El derecho fundamental a…,* op. cit., pp. 236-249; TRONCOSO REIGADO A.: *La protección de datos personales: en busca de su equilibrio,* Tirant lo Blanch, 2011, pp. 171-177.

[69] Recomendación CM/Rec (2015) Comité de Ministros del Consejo de Europa sobre el tratamiento de datos personales en el contexto de empleo, de 1 de abril de 2015, disponible en https://wcd.coe.int/ViewDoc.jsp?id=2306625 [Consulta 30/04/2015]. Esta Recomendación sustituye a la Recomendación (89) sobre la protección de los datos de carácter personal utilizados con fines de empleo, de 18 de enero de 1989.

[70] Esta Recomendación establece algunos consejos para, entre otros, poder realizar pruebas que constaten la aptitud de un candidato para un determinado puesto de trabajo, será necesario el consentimiento del interesado. Lo mismo ocurre cuando lo que se pretende tratar son datos especialmente protegidos, como son aquellos relativos a la salud, estableciendo que sólo podrán someterse a examen médico los trabajadores con el fin de determinar su aptitud para un puesto actual o futuro. Se limita por tanto, la recogida de dichos datos al personal sujeto al secreto médico, pudiendo comunicarlo únicamente cuando resulte indispensable. Respecto de la conservación de los datos, se establece que los datos que han sido presentados para una candidatura a una oferta de empleo deberán suprimirse cuando quede claro que no se va a hacer ninguna oferta. Los aspectos que mayores novedades aportan son aquellos referidos a a regular la protección de los datos personales del trabajador ante la utilización de la tecnología, y utilizo ahora esta palabra en su acepción más amplia, durante su vida laboral, ya sea en la fase previa de acceso al empleo o durante su prestación.

En un documento de trabajo del Grupo del art. 29[71] puede encontrarse una encuesta sobre los problemas relacionados con la protección de datos más comunes en el contexto laboral[72]. A este efecto, el Grupo de trabajo analizó la importancia del consentimiento como base jurídica para el tratamiento de datos de empleo[73]y consideró que el desequilibrio económico, entre el empresario que solicita el consentimiento y el empleado que se lo da, planteará con frecuencia dudas sobre si el consentimiento es o no libre[74], por lo que las circunstancias en las que se solicita el consentimiento deberán considerarse de forma cuidadosa a la hora de valorar su validez en el contexto laboral. Como consecuencia el Grupo redactó un "*Informe y Recomendaciones sobre telecomunicaciones y la privacidad en las relaciones laborales*"[75], en el que se aboga por la protección de los datos de los trabajadores, no sólo en el centro de trabajo sino también en su propio domicilio, debido a la proliferación del denominado teletrabajo[76].

Actualmente, se ha incorporado al derecho comunitario, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se

[71] El denominado Grupo de Berlín (*GRUPO DE TELECOMUNICACIONES DE BERLÍN. International Working Group on Data Protection in Telecommunications: IWGDPT*) se creó en 1983, a iniciativa de la autoridad de protección de datos del Land de Berlín, donde tiene su sede. El Grupo reúne a autoridades de control, procedentes fundamentalmente de países europeos y de América del Norte, junto con representantes de organizaciones internacionales y expertos. Es un foro de trabajo abierto que pretende debatir sobre las implicaciones del uso de las telecomunicaciones en la esfera privada de los individuos, anticipándose a los problemas que se plantean en la práctica.

[72] Grupo del art. 29 (2001), *Dictamen 8/2001 sobre el tratamiento de datos de carácter personal en el contexto laboral*, WP 48, Bruselas, de 13 de septiembre de 2001.

[73] Grupo del art. 29 (2005), *Documento de trabajo relativo a una interpretación común del art. 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995*, WP 114, Bruselas, de 25 de noviembre de 2005.

[74] AGENCIA DE DERECHOS FUNDAMENTALES DE LA UE*: Manual de legislación europea en materia de protección de datos,* 2014, pp. 187-188, disponible en: http://www.echr.coe.int/Documents /Handbook_data_protection_SPA.pdf. [Consulta 20/01/2015].

[75] En dicho documento (Grupo del art. 29, agosto 1996) se informa sobre los /métodos de /recogida de datos más comunes utilizados en el seno de las organizaciones empresariales, dispositivos magnetofónicos, audiovisuales, identificadores de datos biométricos, dispositivos de video vigilancia, etc. Estos medios se tendrán que utilizar de forma proporcionada a la finalidad que lo justifica, por lo que estos trabajadores y sus representantes deberán ser informados del tipo de tecnología utilizada por el empresario para vigilar el desarrollo de la actividad laboral.

[76] PIÑAR MAÑAS, J.: "Protección de datos y relaciones laborales" en FARRIOLS I SOLA, A (COORD): *La protección de datos en los centros de trabajo*, Cinca, 2006, pp. 139-141.

deroga la Directiva 95/46/CE (Reglamento general de protección de datos)[77] que tiene como objetivos centrales los siguientes: adaptar la protección de datos a las nuevas demandas del mundo digital, teniendo en cuenta que las disposiciones vigentes se adoptaron cuando menos del uno por ciento de los ciudadanos europeos utilizaba Internet; evitar las actuales divergencias en la aplicación de las normas sobre protección de datos por parte de los diferentes Estados miembros y velar para que los derechos fundamentales a la protección de datos personales se apliquen de manera uniforme en todos los ámbitos de las actividades de la Unión; aumentar la confianza del consumidor en los servicios en línea facilitando una mejor información con respecto a los derechos y a la protección de datos mediante la introducción del derecho a la rectificación, al olvido y a la supresión, del derecho a la portabilidad de datos y de oposición; impulsar el mercado único digital; la creación de perfiles; la definición de datos seudónimos; la obligatoriedad de incluir premisas de protección de datos en el mismo diseño de los procesos; el desarrollo de un "Sello Europeo de Protección de datos"[78]; el endurecimiento de las sanciones; y, finalmente, cambios en lo relativo a la transferencia internacional de datos.

Este Reglamento no trata de forma específica la protección de datos de trabajadores pero es obvio que puede introducir mejoras en el tratamiento de los mismos ya que va a modificar bastantes aspectos de la normativa española sobre protección de datos relacionados con los servicios en línea, transferencia internacional de datos[79], inclusión de requisitos de privacidad en el diseño de

[77] DOUE nº L 119/1 de 4 de mayo de 2016.
[78] El "Sello Europeo de Protección de Datos" tiene un objetivo principal: "crear confianza entre los interesados". Por tanto, se puede considerar un argumento de valor competitivo en el contexto del mercado único digital europeo que no sólo interesa a las empresas europeas sino también a las de fuera de Europa, en tanto dirijan su oferta de servicios y productos a los europeos. El "sello" podrá ser obtenido tanto por responsables como por encargados del tratamiento, para lo que podrán solicitar a "cualquier autoridad de control de la Unión" que les certifique que el tratamiento de datos personales que llevan a cabo se realiza de conformidad con lo previsto en el Reglamento; lo que se traduce en que se da libertad a los solicitantes para obtener la certificación de cualquier autoridad de protección de datos europea, con independencia de las reglas competenciales que puedan ser de aplicación.
[79] Sobre este aspecto APARICIO SALOM, J. establece que existe una tendencia hacia la personalización, añadiendo el elemento de residencia como criterio de conexión que provoca la aplicación de la norma*: "Esta regla constituye una innovación importante en el régimen de protección de datos, pues tal y como menciona el art. 20 del Reglamento Europeo de Protección de Datos el tratamiento de datos por un responsable de tratamiento no establecido en la Unión debe someterse a lo dispuesto en el presente Reglamento en caso de que las*

productos y servicios, etc. Para reforzar la observancia del derecho a la protección de datos de los trabajadores en la empresa, el Reglamento prevé incrementar la responsabilidad de quienes tratan los datos, exigiendo el nombramiento de un Delegado de Protección de Datos[80].

1.2. Regulación y contenido del derecho a la protección de datos de carácter personal en España.

Como es sabido, la transposición de la Directiva 95/46/CE[81] fue clave para la creación de la actual norma española sobre protección de datos pues, aunque en un principio lo que se propuso era modificar algunos preceptos de la LORTAD para adaptarla a lo establecido en la Directiva 95/46/CE, esto no fue posible y, finalmente, se culminó este proceso con la promulgación de la LOPD la cual, como se verá en este apartado, mantiene una regulación descuidada en algunos aspectos así como ciertos defectos de tipo sistemático[82].

Según el art. 1 de la LOPD, la norma tiene como objetivo "*garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal".* Esta finalidad es distinta, y más amplia, que la establecida en la LORTAD[83] ya que en ésta sólo se establecían limitaciones del uso de la informática como medida para

---

actividades de tratamiento se refieran a la oferta de bienes o servicios a dichos interesados, o al control de su conducta" en *Estudio sobre la protección de datos*, Thomson-Reuters Aranzadi, 2013, pp.57-58.

[80] HERNÁNDEZ LÓPEZ, J.M*.: El derecho a la protección de datos en la Doctrina del Tribunal Constitucional*, Thomson-Reuters Aranzadi, 2013, pp.37-40; APARICIO SALOM, J.: *Estudio sobre la protección*…, op. cit., pp. 287-289.

[81] SÁNCHEZ BRAVO, A: "La Ley orgánica 15/1999, de protección de datos de carácter personal: diez consideraciones en torno a su contenido", *Revista de Estudios Políticos*, núm. 111 (separata), 2001, pp. 203-206; VV.AA: "Y la protección de datos en España cumplió veinte años" *Diario La Ley*, núm. 8031, 2013.

[82] MURILLO DE LA CUEVA, P.L.: "Las vicisitudes del Derecho de la protección de datos personales", en VV.AA: *La democracia constitucional: estudios en homenaje al profesor Francisco Rubio Llorente.* (vol. I) Centro de Estudios Políticos y Constitucionales, Madrid, 2003, pp. 513-515; TÉLLEZ AGUILERA, A.: *Nuevas tecnologías. Intimidad y protección de datos*. Edisofer, 2001, pp.107-109.

[83] Art. 1.1 LORTAD*: "La presente Ley Orgánica, en desarrollo de lo previsto en el apartado 4 del art. 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos".*

salvaguardar la intimidad, personal y familiar del individuo. En cambio, en la LOPD se concibe la informática como herramienta del progreso social, razón por la que no debe estar limitada, aunque sí que debe conectarse su uso con la necesidad de garantizar la protección de los datos de carácter personal. Con esta afirmación no se quiere decir que las TICS no sean un instrumento lesivo de los derechos del individuo, que como es obvio pueden serlo, si bien en la nueva LOPD se intenta equilibrar el uso legítimo de estos mecanismos con el ejercicio del derecho a la protección de datos[84].

La nueva regulación de la protección de datos personales viene a solucionar algunas de las deficiencias contenidas en la derogada LORTAD, entre otras, el establecimiento de una serie de conceptos que antes no eran contemplados tales como el de fuente accesible al público, encargado del tratamiento de datos, etc.; pero, a su vez, se configura como una norma llena de excepciones y de remisiones a otros textos normativos de desarrollo. Así, por ejemplo, es conveniente destacar el diferente trato al que están sometidos los ficheros según sean de titularidad pública o privada, sobre todo en cuanto a las excepciones respecto de los primeros[85], ofreciendo a los ciudadanos una protección menos eficaz y permitiendo que en este tipo de ficheros se puedan producir más quebrantos en su derecho a la protección de datos de carácter personal[86].

---

[84] En este sentido: APARICIO SALOM, J: *Estudio sobre la protección*…, op. cit., pp. 21-22; LESMES SERRANO, C (coord.): *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia,* Lex Nova, 2008, pp. 48-49.

[85] Art. 23 de la LOPD: *"1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del art. anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado está siendo objeto de actuaciones inspectoras.3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación".*

[86] SANTOS GARCÍA, D.: *Nociones generales dela Ley Orgánica de Protección de datos y su Reglamento*, Tecnos, 2012, pp. 173-175; TÉLLEZ AGUILERA, A.: *Nuevas tecnologías, intimidad…,* op. cit., pp. 109-111; PÉREZ VELASCO, M.M.: "Los ficheros públicos" en TRONCOSO REIGADA, A.

Por otra parte, se sigue optando, como ocurría en la LORTAD, por un sistema mixto, es decir, se permite la remisión a normas de carácter sectorial para regular aspectos específicos de la protección de datos de carácter personal. No obstante, en lo que a la gestión de los datos de los trabajadores se refiere, no existe, como se ha apuntado, una normativa especial, remitiendo la solución de estos conflictos a la normativa general de protección de datos. Es necesario afirmar que las normas sectoriales existentes sobre la protección de datos de carácter personal tienen que respetar los criterios establecidos en la LOPD que, como se sabe, es una legislación de carácter general aplicable a todas las personas físicas, sin atender al ámbito en el que se pueda ver alterado su derecho[87]. Pues bien, la LOPD permite la dispersión normativa dejando pasar la ocasión de establecer la unidad legislativa del sistema. Con este planteamiento, el legislador consiente la coexistencia de otras normas con la general[88], no desarrollándose, con este hecho, el mandato introducido por el art. 18.4 CE, el cual parece pretender la elaboración de una ley de aplicación global[89] que pueda dar respuesta a todas las situaciones que puedan plantearse en relación con la privacidad de los ciudadanos[90].

(coord.): *Estudios sobre Administraciones Públicas y Protección de datos personales,* Thomson-Civitas, 2006, pp. 117-119.

[87] Art. 2.3 de la LOPD: "*Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales: a) Los ficheros regulados por la legislación de régimen electoral. b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública. c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas. d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes. e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia".*

[88] Al contrario de lo que ocurre en Francia, dónde la norma sobre protección de datos somete a todos los tratamientos, incluso a los anteriores a ella, a sus disposiciones y no contempla regímenes especiales ni excepciones, tal y como establecen los arts. t. 15, 16 y 17, vid. TÜRK, A.: *La ley francesa de protección de datos de carácter personal*, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/ConferenciaTURK.pdf. [Consulta 20/01/2015].

[89] En Alemania (Ley federal de protección de datos de 14 de enero de 2003, publicada en BGBI I, S. 66) son frecuentes las remisiones a otras disposiciones sobre protección de datos. Véase a este efecto, el art.1: "*Siempre que otras disposiciones legales o reglamentarias federales, fueren aplicables a datos personales, incluida su publicación, prevalecerán sobre las disposiciones de la presente ley, sin perjuicio de la obligación de observar deberes legales de secreto, o de secreto profesional o de secreto oficial que no se fundaren en disposiciones legales".* El ejemplo más claro de la utilización de leyes sectoriales, aunque se aparte de la presente exposición, basada esencialmente en norma europeas, , es el caso americano que se

En cuanto al contenido del derecho a la protección de datos, se hace preciso distinguir entre lo que se entiende por acceso y tratamiento de datos de carácter personal, ya que no se puede tratar de la misma manera el simple acceso a un dato que el procesamiento de información de la forma establecida en art. 3 c) de la LOPD. Es más, la Directiva 95/46/CE tampoco considera tratamiento el simple acceso a los datos pues establece que se tienen que dar alguno de los usos definidos[91] para que los datos estén dentro del ámbito de su protección. Efectivamente, al igual que pasa en la LOPD, el acceso a los datos, para la Directiva 95/46/CE, nada tiene que ver con el tratamiento, aunque se puede considerar que son dos acciones estrechamente relacionadas ya que una de las formas de acceder a los datos puede ser su conocimiento a través de los ficheros dónde se encuentren almacenados, sin considerarse este acceso tratamiento a menos que, una vez que se conozca la información personal, concurran alguna de las actuaciones catalogadas en el art. 3 c) de la LOPD. Incluso, en los Estándares Internacionales sobre protección de datos personales y privacidad aprobados el 9 de noviembre de 2009 en la Conferencia Internacional (Madrid) se aboga por que el tratamiento de datos se haga de forma estructurada, sin que en ellos se mencione el término fichero, aunque pueda deducirse por la definición dada[92].

---

presenta como un modelo legislativo de protección de datos basado en un conjunto de leyes sectoriales antes que en una ley general. Vid. Sobre este asunto: PÉREZ LUÑO, A.E.: "El derecho a la autodeterminación informativa", en *II Jornada de Estudio sobre "Protección de datos y Derechos fundamentales*" Servicios de Estudios del IVAP, 1991, pág.313.; HEREDERO HIGUERAS, M.: "La nueva Ley alemana federal de protección de datos". *Boletín Oficial del Ministerio de Justicia*, núm. 1630. pág.130, disponible en http://www.mjusticia.gob.es/cs/ [Consulta 21/01/2015].

[90] SERRANO PÉREZ, M.M.; *El derecho fundamental a la protección de datos. Derecho español y comparado*, Thomson-Civitas, 2003, pp. 113-114.

[91] Art. 2 b) Directiva 95/46/CE*: "Tratamiento de datos personales: cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción".*

[92] Vid., punto 3 de los Estándares Internacionales sobre protección de datos personales y privacidad disponible en https://secure.edps.europa.eu /EDPSWEB/webdav/ site/mySite/shared /Documents/Cooperation/Conference_int/09-11-05_Madrid_Int_standards_ES.pdf [Consulta 26/04/2015].

Por este motivo, si se sigue lo establecido en la LOPD, parece lógico pensar que la simple visualización de información personal no siempre tiene que conllevar el almacenamiento o la recogida de datos en un fichero determinado, como por ejemplo puede suceder cuando se envía un email con datos de un trabajador, a efectos informativos, sin que se archive el correo electrónico. Ahora bien, cabe hacer una matización pues en el art. 5.1 t) del RDLOPD[93] se contempla la consulta entre las posibles acciones que pueden dar lugar a un tratamiento de datos, sin dejar claro qué se puede entender por esta actuación y si ésta se puede equiparar entonces un acceso a los datos[94]. No obstante, en la LOPD tan sólo se habla de acceso para referirse a situaciones en las que ese conocimiento de los datos sea por parte de terceras personas y siempre que se realice por cuenta del responsable del tratamiento[95]. Por otra parte, esta ausencia de ordenación puede provocar situaciones en las que los datos queden desprotegidos ya que es difícil comprobar si el que accede o visualiza esa información no acaba realizando finalmente un tratamiento[96].

De forma general, integran el contenido activo del derecho a la protección de datos de carácter personal las siguientes facultades: 1) ser informado de la recogida de datos; 2) conocer la existencia de ficheros y tratamientos de datos personales; 3) acceder a ellos para comprobar qué información personal contienen; 4) obtener la rectificación de los que no sean exactos; 5) obtener la cancelación de los que no deban ser tratados o hayan

[93] Art. 5.1 t) RDLOPD: "*Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencia".*

[94] En este sentido se puede concluir, para tratar de entender el concepto de acceso y su implicación en la normativa sobre protección de datos, que el acceso se considera en la mayor parte de las opiniones doctrinales y jurisprudenciales, como se verá, como un elemento previo a la utilización y tratamiento del dato. Por lo que se concibe como una acción que posibilita el tratamiento de datos sin estar integrada en la realización del mismo.

[95] Vid., art. 12.1 LOPD.

[96] Ese acceso puede acarrear que el usuario que conoce esos datos, en primera instancia, pueda tomar nota de los mismos o incluso informatizarlos, a través de la introducción de la información en una base de datos de la empresa. Es muy sencillo memorizar algunos datos a partir de una mera visualización del CV, sobre todo, si el traspaso o la escritura de los mismos se realiza en un momento inmediatamente posterior al citado acceso. Con esto se quiere decir que el acceso debería estar contemplado en la norma, pues se puede atentar contra el derecho a la protección de datos si el acceso no se realiza de forma correcta o transgrede el alcance del simple visionado.

perdido la calidad que en su día justificó el tratamiento; 6) no sufrir perjuicios como consecuencia de decisiones tomadas exclusivamente en virtud de perfiles personales obtenidos informáticamente; 7) ser resarcido de los perjuicios sufridos a causa de tratamientos que no se ajusten a las condiciones legalmente establecidas; 8) ser protegido por las instituciones especializadas creadas *ex profeso* para defender este derecho fundamental[97].

Como complemento de este contenido hay que tener en cuenta la definición de fichero de dato de carácter personal[98] así como distinguir entre fichero público y privado, pues el procedimiento de creación tiene requisitos distintos dependiendo de la catalogación que se le dé a la base de datos. Así, para la constitución de un fichero de carácter privado no se exige ningún requisito adicional, tan solo su notificación y registro en la AEPD; sin embargo, si la naturaleza del fichero es pública, su configuración, modificación o supresión solo podrá hacerse por medio de una disposición general publicada en el BOE, como establece el art. 20 de la LOPD[99].

Determinado el concepto de fichero de datos de carácter personal y su tipología, es conveniente subrayar la importancia de las figuras de responsable del fichero y de encargado de tratamiento, cuya delimitación se desarrollará de forma más específica cuando se haga referencia al procesamiento de datos.

---

[97] MURILLO DE LA CUEVA, P.L.: "Perspectivas del derecho a la autodeterminación informativa" *Revista Indret*, núm. 5, 2007, pág. 20; SANTOS GARCÍA, D.: *Nociones generales de la…,* op. cit., pp. 31-33; PRIETO GUTIÉRREZ, J.M.: "Objeto y naturaleza jurídica del derecho fundamental de protección de datos", *Boletín del Ministerio de Justicia*, núm.1971-1972, 2004, pp. 3119-3146.

[98] Art. 3 b): "*Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".*

[99] Sobre este aspecto, a título de ejemplo, es preciso resaltar el caso de Francia dónde se hace necesaria la autorización del CNIL (Comisión Nacional de Informática y Libertades) para el tratamiento de datos realizado por entes públicos, como así se desprende del art. 15 de la normativa francesa sobre protección de datos donde sólo se exige una declaración con carácter previo a la puesta en funcionamiento de todos aquellos ficheros que no están comprendidos en el citado art. 15. En Portugal se distingue entre ficheros con datos sensibles y aquéllos que no contienen este tipo de informaciones, estableciendo de forma genérica la autorización o registro para cualquier fichero unida al dictamen de la CNPD (Comisión Nacional de Protección de Datos); así lo establece el art. 7.2 de la Lei núm. 67/98, de 26 de outubro, de datos personales (Diario de la República I Serie A núm. 247): "*Mediante disposição legal ou autorização da CNPD, pode ser permitido o tratamento dos dados referidos no número anterior quando por motivos de interesse público importante ese tratamento for indispensável ao exercício das atribuições legais ou estatutárias do seu responsável, ou quando o titular dos dados tiver dado o seu consentimento expresso para ese tratamento, em ambos os casos com garantias de não discriminação e com as medidas de segurança previstas no artigo 15".*

La definición de estos sujetos viene establecida en los arts. 3 d) y 3 g) de la LOPD[100], siendo necesario su conocimiento por parte de los ciudadanos y trabajadores para que puedan ejercer los derechos que les confiere la normativa sobre protección de datos (acceso, oposición, cancelación y rectificación).

Otro de los aspectos que merece la pena destacar es el referido al concepto de fuentes accesibles al público, un tema polémico ya que en la LORTAD no se especificó que fuentes eran de acceso público y cuáles no; aspecto que se ha intentado solucionar en la LOPD estableciendo un "*numerus clausus"* de las mismas[101]. En cuanto a la gestión de datos efectuada por las entidades encargadas de ese cometido, tanto en el acceso al empleo como durante la relación laboral, se puede decir que los datos que constan en estas fuentes y cuyo conocimiento puede ser interesante para su actividad son aquéllos que obran en las listas profesionales -nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo, estando autorizados para acceder a esta información[102], siempre que no haya una norma limitativa que lo prohíba[103].

---

[100] Art. 3.d) de la LOPD: *"Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento"*. Art. 3.g) de la LOPD: *"Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".*

[101] Art. 3.j) de la LOPD: "*Fuentes de datos accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación".*

[102] Esta información de los trabajadores que aparece en las denominadas listas profesionales podrá ser tratada sin consentimiento del titular del dato ya que este consentimiento está exceptuado para el procesamiento de estos datos obrantes en fuentes accesibles al público (art. 6.2 LOPD).

[103] Cualquier información que exceda de la prevista en el art.3 j) de la LOPD precisará el previo consentimiento del titular del dato para el tratamiento de esos datos, pues no podría tener, entonces, la consideración de fuente accesible al público. En este sentido, la Sentencia de la Audiencia Nacional de 4 de febrero de 2013 (JUR 2013\61765) establece que: "*Consta en la resolución que con la prueba denegada no se trataba de saber si el documento en cuestión había sido elaborado por el Ayuntamiento o por el organismo autónomo en cuestión que ya está aclarado en el folio número 89 por la Secretaria e interventora, sino que lo determinante era conocer si los datos personales que aparecían en este cuadro, singularmente la asociación*

Como es sabido, la LOPD fue desarrollada en un principio por el Real Decreto 994/1999, de 11 de junio, por el que se aprobó el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal[104], norma derogada por el Real Decreto 1720/2007, de 21 de diciembre[105], en el que, además de otras materias, se regula todo lo referente a las medidas de seguridad de los ficheros de datos de carácter personal. Por ejemplo, en cuanto al ámbito de aplicación, una de las principales novedades que introduce el RDLOPD es la inclusión de las medidas de seguridad a adoptar respecto no sólo de los ficheros automatizados, sino también de los no automatizados. También se determina el ámbito territorial de la norma, circunscribiéndolo no sólo a todo tratamiento de datos de carácter personal realizado en territorio español, sino abarcando también los datos que trasciendan nuestras fronteras con la contemplación de la transferencia internacional de datos[106]. Del mismo modo, se hace mención expresa a la figura del encargado del tratamiento y se regula el ejercicio del derecho de oposición del afectado; y también se tratan las indemnizaciones que podrá percibir el perjudicado que sufra daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto en la LOPD por el responsable o el encargado del tratamiento.

---

entre nombre y apellidos de trabajadores, puestos de trabajo desempeñados, y salarios asignados a esos puestos, provenían o no de una fuente accesible al público. Y asimismo consta en la resolución que no se ha acreditado que figuren en fuentes accesibles al público de acuerdo con el art. 3, j), de la Ley de Protección de Datos, y que durante todo el procedimiento se ha aportado toda la documentación que se ha considerado oportuna para su defensa…. se confirmó la sanción impuesta, por la difusión en un folleto de datos personales -nombre y apellidos junto a las retribuciones- del personal de un Ayuntamiento, que son datos que no figuran en un Boletín Oficial, así asociados -como es el presente caso-, cuya publicación no se deriva de la regulación local, y sin que pueda considerarse fuente accesible al público la publicación de los mismos en su caso en un tablón del Ayuntamiento, ni están amparados por la información política".

[104] BOE núm. 151, de 25 de junio de 1999.

[105] BOE núm. 17, de 19 de enero de 2008.

[106] Art. 66 del RDLOPD: *"Para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el art. 70 del presente reglamento".*

Entre las novedades más destacadas del RDLOPD se encuentran además: la ampliación del conjunto de definiciones recogidas en la LOPD[107]; la fijación del criterio que hay que seguir respecto al cómputo de plazos sin prestar atención a si el fichero es de titularidad pública o privada; la especial importancia que se le da a la figura del encargado del tratamiento; la concreción en cuanto a los procedimientos para obtener el consentimiento del titular de los datos; la importancia del documento de seguridad, etc. La aprobación del RDLOPD y la recopilación de todos los criterios citados en el texto hacen que se reflejen los elementos interpretativos más sobresalientes respecto de lo establecido en la LOPD, dotando a ésta de una seguridad jurídica que no existía hasta la promulgación del citado Reglamento. Además, se intenta simplificar el procedimiento de notificación de ficheros de datos de carácter personal al Registro General de Protección de Datos (RGPD), estableciéndose que, para la cesión de datos de carácter personal, se deberá informar al afectado de la finalidad de la cesión y del tipo de actividad del cesionario[108].

2. LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL COMO DERECHO FUNDAMENTAL Y AUTÓNOMO.

Aunque es evidente, que el objeto central del presente trabajo no es la configuración de la protección de datos como derecho fundamental, es importante hacer algunas matizaciones en este sentido para explicar brevemente, no sólo su categorización, sino también su autonomía respecto al derecho a la intimidad.

[107] La norma incluye en el apartado de definiciones (art.5 del RDLOPD) algunos conceptos que no estaban contemplados en el art. 3 de la LOPD, encargado de establecer el listado de aspectos conceptuales de la norma. Estas inclusiones son las referidas a: cancelación del dato; dato disociado; exportador de datos personales; fichero de titularidad pública y privada, destinatario o cesionario; etc.

[108] ORTEGA GIMÉNEZ, A.: "El derecho fundamental a la protección de datos de Carácter Personal en España", *AR. Revista de Derecho Informático*, núm. 121, 2008. pág. 11; VELEIRO REBOREDO, B.*: Protección de datos de carácter personal y sociedad de la información,* Estudios Jurídicos Boletín Oficial del Estado, 2008, pp. 42-44; MARTÍNEZ MARTÍNEZ, R.: *Protección de datos: Comentarios al reglamento de desarrollo de la LOPD*, Tirant lo Blanch, Valencia, 2009, pp.80-87 y 121-125.

En un primer momento, su reconocimiento como derecho fundamental tuvo lugar por la Sentencia del Tribunal Constitucional 254/1993, de 20 de julio[109]. En la citada Sentencia, el demandante pretendía que la actuación del Gobernador Civil de Guipúzcoa fuera declarada contraria a los arts. 18.1 y 18.4 de la CE, pues se le denegaba la información que el actor había solicitado acerca de sus datos de carácter personal que obraban en ficheros automatizados de la Administración del Estado. La reclamación del demandante y titular de los datos de carácter personal estaba fundada en la falta de explicaciones relativas a la finalidad pretendida por el fichero de datos automatizado de la citada Administración Pública. Como su solicitud no fue atendida por la Administración, pues no contestó a su requerimiento, el afectado decidió interponer recurso de amparo ante el Tribunal Constitucional, el cual reconoció la existencia de un derecho directamente derivado de la aplicación del art. 18.4 de la CE, denominado derecho a la libertad informática que califica como un derecho en sí mismo pero sin considerarlo plenamente autónomo y desvinculado del derecho a la intimidad[110].

En consecuencia, el Alto Tribunal incorpora una nueva garantía constitucional que procura dar respuesta a los ataques producidos a la intimidad, sobre todo si se utilizan los datos personales para finalidades distintas a las establecidas previamente, estando la información a la que se

[109] RTC 1993\254.

[110] Para el reconocimiento del derecho como fundamental, la Sentencia 254/1993 del Tribunal Constitucional establece que*: "Ahora bien, a esa ausencia de legislación no se pueden enlazar las desmesuradas consecuencias que postula el Abogado del Estado. Aun en la hipótesis de que un derecho constitucional requiera una interpositio legislatoris para su desarrollo y plena eficacia, nuestra jurisprudencia niega que su reconocimiento por la Constitución no tenga otra consecuencia que la de establecer un mandato dirigido al legislador sin virtualidad para amparar por sí mismo pretensiones individuales, de modo que sólo sea exigible cuando el legislador lo haya desarrollado. Los derechos y libertades fundamentales vinculan a todos los poderes públicos, y son origen inmediato de derechos y obligaciones, y no meros principios programáticos... Ahora bien, la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaria, y es aquí donde pueden venir en auxilio interpretativo los tratados y convenios internacionales sobre esta materia suscritos por España. Pues, como señala el Ministerio Fiscal, la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada «libertad informática» es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático*". A pesar de ser esta la opinión mayoritaria del TC, en esta sentencia, merece la pena destacar el voto particular emitido por el ponente Miguel Rodríguez-Piñero Bravo-Ferrer, el cual señala que no se puede utilizar el Convenio núm. 108 del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal como un elemento de integración ante la demora en el desarrollo legislativo del art. 18.4 CE.

refiere esta Sentencia almacenada en un fichero automatizado, conectando la protección de datos con el uso de la informática y reconociendo, de este modo, el derecho a la libertad informática: "*En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática*[111]*".*

Aunque la Sentencia reconoce expresamente la existencia de un derecho a la libertad informática, su configuración definitiva como derecho fundamental[112] se encuentra en la Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre[113], al diferenciar los derechos contenidos en el art. 18.1 y en el art. 18.4 hasta el punto de considerar que "*el derecho a la*

[111] Como señala GARRIGA DOMÍNGUEZ, A. "*la problemática que suscita el tratamiento automatizado de la información personal es tan singular, que requiere una solución jurídica ad hoc, de un nuevo instrumento de tutela y garantía de la libertad y dignidad humanas",* en *Tratamiento de datos personales y derechos fundamentales*, Dykinson, 2009, pág. 30; ÁLVAREZ CIENFUEGOS, J.M., en temprano Comentario a las Sentencias 290 (RTC 2000, 290) y 292/2000 (RTC 2000, 292) , ha llamado la atención sobre este punto. Véase su estudio sobre "La Libertad Informática, un nuevo Derecho Fundamental en nuestra Constitución", *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía,* núm. 1, 2001, pp. 1724-1731; CAMPUZANO LAGUILLO, A.B.: "Algunas consideraciones sobre la libertad informática y el derecho a la protección de datos de carácter personal en la jurisprudencia constitucional", *Revista Aranzadi de derecho y nuevas tecnologías*, núm. 1, 2003, pp. 99-103; ORTÍ VALLEJO, A.: "El nuevo derecho fundamental (y de la personalidad) a la libertad informática (A propósito de la STC 254/1993, de 20 de julio)" *Derecho privado y Constitución*, núm. 2, 1994, pp. 305-310; SÁNCHEZ BRAVO A*.: La protección del derecho a la libertad informática en la Unión Europea*, Universidad de Sevilla, 1998, pp. 42-47.

[112] En otros países europeos también se ha configurado la existencia del derecho fundamental a la protección de datos de carácter personal en sede jurisprudencial; tanto es así que la discusión en Italia sobre la existencia de un derecho a la protección de datos de carácter personal tiene su configuración definitiva, al igual que sucede en España, en la doctrina constitucional, pues es el Tribunal Constitucional, en la Sentencia de 27 de mayo de 1975 n.2129, el que establece definitivamente la existencia de un derecho autónomo a la vida privada, como es el "*diritto a la riservatezza"* y realiza un primer intento de delimitación del contenido positivo del derecho introduciendo el concepto de *"interés social a la información"*. También en Alemania el derecho a la autodeterminación informativa es reconocido por el Tribunal Constitucional Federal en su Sentencia de 15 de diciembre de 1983, dónde se reconoce la base y los elementos esenciales del contenido de este derecho. Vid.: MARTINOTTI, G.: "Privacy e statuto dell'informazione" *Banchedati, telemática e diritti della persona,* Cedam, 1984. pp. 201; RODOTA, S.: "Privacy e construzione della sfera privata. Ipotesi e prospettive" *Política del diritto*, núm.4, 1991; GARRIGA DOMÍNGUEZ, A.: *Tratamiento de datos personales…,* op. cit*.,* pág. 31; BRU CUADRADA, E.: "La protección de datos en España…", op. cit., pp. 81, 86; SERRANO PÉREZ, M.M: *El derecho fundamental…,* op. cit., pp.60-63.

[113] RTC 2000\290.

intimidad no aporta por si sólo una protección diferente frente a esa nueva realidad derivada del progreso tecnológico"[114]*.* No obstante, la Sentencia parece certificar la existencia de un derecho a la autodeterminación informativa[115] ya que, aunque el control del tráfico de los datos personales adquiere más importancia en el marco de las nuevas tecnologías, quizás la autodeterminación informativa sea un concepto más apropiado pues extiende su protección a aquellos datos que se encuentren en cualquier tipo de soporte. En todo caso, esta resolución jurisprudencial refuerza el criterio seguido por la Sentencia 254/1993 constituyendo un avance respecto de ella al considerar el derecho a la libertad informática como derecho fundamental autónomo.

Evidentemente, la calificación del derecho a la autodeterminación informativa o derecho a la protección de datos[116] como autónomo tiene como objetivo dotar al titular del dato de una serie de facultades que le permitan disponer de su información personal, hasta el punto de no sólo restringir su acceso y tratamiento a las personas autorizadas por él, sino también saber en todo momento cuál va a ser el destino y el uso de sus datos. La declaración de autonomía e independencia del derecho se consolida en la Sentencia

[114] Especial interés merece el análisis realizado por el voto particular de JIMÉNEZ DE PARGA, relativo al reconocimiento de la independencia o autonomía del derecho a la protección de datos. El Magistrado basa su discrepancia con la Sentencia en la fundamentación de este nuevo derecho pues, mientras que la STC 290/2000 configura el nuevo derecho fundamental partiendo del art. 18.4 CE, a su juicio este precepto no es más que un simple mandato al legislador para limitar el uso de la informática, por lo que entiende que el fundamento de su existencia debe estar justificado en el derecho a la dignidad de la persona*: "A mi entender, la libertad informática, en cuanto derecho fundamental no recogido expresamente en el texto de 1978, debe tener como eje vertebrador el art. 10.1 CE, ya que es un derecho inherente a la dignidad de la persona. Tal vinculación a la dignidad de la persona proporciona a la libertad informática la debida consistencia constitucional. También son preceptos que facilitan la configuración de la libertad informática los contenidos en los arts. 18.1 (derecho al honor, a la intimidad personal y familiar y a la propia imagen) y 20.1 (libertad de expresión y de información) (…)".*

[115] Sentencia 290/2000 del TC de 30 de noviembre (RTC 290/2000) que, tras una extensa consideración sobre la realidad del avance tecnológico y sus riesgos para con los derechos de la persona y su más eficaz garantía, entiende que es expresión de esta nueva realidad y de la preocupación suscitada un nuevo derecho fundamental que ha venido a denominarse derecho fundamental a la autodeterminación informativa.

[116] Del pronunciamiento de la Sentencia 292/2000, de 30 de noviembre, no se desprende, sin embargo, una distinción de ambos conceptos. A lo largo de la Sentencia se utilizan indistintamente las dos nociones, configurándose el derecho a la autodeterminación informativa como la decisión personal de determinar lo que cada uno quiere que los demás conozcan de nuestra persona, y el derecho a la protección de datos como el instrumento necesario para garantizar a esa persona ese espacio de protección.

292/2000, de 30 de noviembre, del Tribunal Constitucional[117], la cual constituye el verdadero eje interpretativo de la protección de datos conformando el contenido de este derecho y configurando los elementos de distinción respecto al derecho a la intimidad[118], a pesar de compartir con él un objetivo común que radica en "*ofrecer una eficaz protección constitucional de la vida privada personal y familiar*[119]*".* El contenido de la Sentencia, en lo relativo a la definición y configuración del derecho a la protección de datos, se centra en lo establecido en los fundamentos jurídicos 6[120] y 7[121] en los que, por un

[117] RTC 2000\292: "*De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede ese tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso".*

[118] RODRÍGUEZ PALENCIA, A.: "La protección de datos en el ámbito de la relación jurídico-administrativa", *Anuario de la Facultad de Derecho de la Universidad de Alcalá,* núm. 2, 2009, pp. 373-375*;* PALOMAR OLMEDA, A.: "La encrucijada de la regulación de la protección de datos", *Actualidad Jurídica Aranzadi,* núm. 804, 2010, pp.1-2; SANTOS GARCÍA, D.: *Nociones generales de la…,* op. cit., pp. 35-37; DEL CASTILLO VÁZQUEZ, I.C.: *Protección de datos: cuestiones constitucionales y administrativas*, Thomson-Civitas, 2007, pp. 305-315.

[119] En este sentido la doctrina ha defendido esa diferenciación, pero sin desligar totalmente el nuevo derecho del derecho a la intimidad. Tanto es así que GUERRERO PICÓ es partidaria de esa autonomía sosteniendo su postura en que "*la necesaria reformulación del derecho a la intimidad no oscurece el reconocimiento de la autonomía dogmática del derecho a la protección de datos de carácter personal"* en *El impacto de Internet en el derecho a la protección de datos de carácter personal*, Thomson-Civitas, 2006, pp.194-207; ALGUACIL GONZÁLEZ-AURIOLES defiende la utilidad de interpretar el art. 18.4 CE en conexión con el art. 18.1 CE, en: "La libertad informática: aspectos sustantivos y competenciales (SSTC 290 y 292/2000)",*UNED, Teoría y Realidad Constitucional*, núm.7, 2001, pág. 371; SERRANO PÉREZ, subraya que no puede ignorarse el papel desempeñado por el derecho a la intimidad en el desarrollo de la protección de datos, pero sí que hay que "*rechazar su identificación con ella por entender que los espacios tutelados por ambos no recaen sobre la misma realidad jurídica"* en *El derecho fundamental…*, op. cit., pág. 483. Otros sectores han querido denotar la independencia de este derecho haciendo referencia a la intención constitucional de que la intimidad estuviera separada de la protección de datos, al configurar un nuevo apartado distinto (art. 18.4 CE) del que regula el derecho a la intimidad (art. 18.1 CE) en DEL CASTILLO VÁZQUEZ, I.C.: *Protección de datos: cuestiones…,* op. cit., pp. 302-304; PULIDO QUECEDO, M.: "¿Numerus clausus o numerus apertus en materia de derechos fundamentales?: el derecho fundamental a la protección de datos", *Repertorio Aranzadi del Tribunal Constitucional*, núm. 20, 2000, pp. 1714-1720.

[120] FJ. 6 STC 292/2000 de 30 de noviembre: "*En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio [RTC 1999, 134] , F. 5; 144/1999, F. 8; 98/2000, de 10 de abril [RTC 2000, 98] , F. 5; 115/2000, de 10 de mayo [RTC 2000, 115] , F. 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios*

lado, se reconoce el citado poder de disposición de los datos por parte de su titular y, por otra parte, se fijan las directrices para que el titular del dato materialice su facultad de control de sus datos personales, tales como: el consentimiento en la recogida del dato; el derecho a saber quién tiene esa información personal; el acceso a esos datos; el derecho a oponerse a ese uso y posesión, etc.

Una vez fijado el contenido del derecho a la protección de datos se pueden establecer las siguientes distinciones respecto al derecho a la intimidad: en primer lugar, la funcionalidad del derecho a la intimidad es defensiva frente a la activa o de disposición relativa a la protección de datos[122]; en segundo lugar, hay que analizar el objeto de cada derecho, puesto que el derecho a la intimidad garantiza a la persona un ámbito reservado de su vida vinculada al respeto de su dignidad como persona y, en cambio, el derecho a la protección de datos extiende su garantía no sólo a la intimidad, sino a todo tipo de dato personal, íntimo, privado o público; y finalmente, el derecho a la intimidad le confiriere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en su esfera íntima así como la prohibición de hacer uso de lo conocido, mientras que la protección de datos garantiza la privacidad de los datos cuando estos han sido sometidos a cualquier tipo de tratamiento, plasmando esta acción en el derecho del

datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin".

[121] FJ.7 STC 292/2000 de 30 de noviembre: "*De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos".*

[122] SAN MARTIN ALCÁZAR, M.T.: "La protección de datos: el nuevo derecho fundamental del siglo XXI", *Revista Jurídica de la Comunidad de Madrid*, núm. 10, 2001, pp.120-121.

afectado a consentir y a ser informado del uso y destino de su información personal[123].

Según lo establecido por el Tribunal Constitucional en las STCS 290/2000 y 292/2000[124] es preciso atender a algunos principios como son: el de autodeterminación informativa, con el que la persona puede decidir qué datos personales proporciona y qué datos puede ese tercero recabar; el del consentimiento en la recogida de los datos; el de ser informado sobre el uso de los datos y la disposición de los mismos; el de oposición a esa posesión por tercero; el de requerir al titular para que rectifique o cancele sus datos, etc. En definitiva la Sentencia concluye que el derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos que sean relevantes o que tengan incidencia en el ejercicio de cualquiera de los derechos de la persona, sean o no derechos constitucionales, y sean o no relativos al honor, la ideología, la intimidad personal y familiar o a cualquier otro bien constitucionalmente amparado[125].

[123] VV.AA: "Vigilar y trabajar: Una aproximación metodológica sobre la intimidad del trabajador como límite de las facultades de vigilancia y control del empresario. A propósito de las SSTCO 98/2000*,* de 10 abril y 186/2000*,* de 10 julio", *Anuario de la Facultad de Derecho de la Universidad de La Coruña,* núm.5, 2001, pág. 889; VV.AA.: *Veinte años de jurisdicción constitucional en España,* Tirant lo Blanch, 2002, pp. 118-120; HERNÁNDEZ LÓPEZ, J.M.: *El derecho a la protección…,* op. cit., pp. 27-33.

[124] Nótese la confusión existente en la doctrina relativa al contenido de las Sentencias 290/2000 y 292/2000, por lo que, para clarificar este asunto es de suma importancia establecer que, como se ha dicho, la Sentencia 290/2000 es la que configura la existencia del derecho fundamental a la autodeterminación informativa, aunque también menciona aspectos de su contenido (véase FJ 7), mientras que la Sentencia 292/2000 establece nuevamente el contenido del derecho (véase FJ 6) pero a raíz de su desvinculación del derecho a la intimidad y sus límites (véase FJ 11).

[125] TRONCOSO REIGADA, A; *La protección de…,* op. cit., pp. 111-132; OROZCO PARDO, G: "La protección de datos en Derecho español a la luz de la reciente jurisprudencia constitucional", *Actualidad Civil*, núm.1, 2002, pp. 220-236; CANALES GIL, A; "La protección de datos como derecho fundamental", *Revista Jurídica de Castilla y León,* núm. 16, 2007, pp. 21-26; GALÁN JUÁREZ, M.: "Comentario de la Sentencia 292/2000 de 30 de noviembre. Protección de datos de carácter personal. Los derechos civiles individuales" en DORREGO DE CARLOS, A.:*25 años de Jurisprudencia Constitucional*, Grupo Difusión, 2007, pp. 117-122; VVAA; *La protección de datos y sus mundos,* DAPP, 2009, pp. 38-40; PIÑAR MAÑAS J.L; "*Protección de datos: origen, situación actual y retos de futuro"* en MURILLO DE LA CUEVA*,* P.L.: *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, 2009, pp. 142-143; SERRANO PÉREZ, M.M; *El derecho fundamental…,* op. cit., pp. 251-255*;* ROIG, A; *Derechos fundamentales y tecnologías de la información y de las comunicaciones*, Bosch, 2010, pp. 11-19; MURILLO DE LA CUEVA, P.L.: "Las vicisitudes del Derecho…", op. cit., pp. 519-520.

En definitiva, el derecho a la protección de datos se configura como un derecho independiente con su propio valor jurídico, de forma que la vulneración del derecho a la protección de datos no tiene por qué suponer un atentado contra el derecho a la intimidad y viceversa, separando también las posibles medidas que se puedan tomar al respecto. Es decir, que se puede presentar una reclamación por infracción del derecho a la protección de datos, sin que esto suponga reclamación por violación del derecho a la intimidad. Por ejemplo, si el titular del dato contenido en un fichero de datos averigua que ese dato está siendo utilizado con otra finalidad, podría denunciar el incumplimiento de la LOPD; pero, sin embargo, si ese dato no está archivado, no entraría dentro del ámbito de protección de la normativa sobre protección de datos y, por tanto, se estaría atentando en su caso contra el derecho a la intimidad si esa información pertenece a su ámbito privado.

2.1. El derecho a la protección de datos como derecho fundamental inespecífico.

Es algo admitido hoy, que los derechos fundamentales que tienen los ciudadanos pueden ser ejercidos de forma universal[126]. Con esta declaración, se establece que estos derechos podrán ser ejercidos por las personas en todos los ámbitos de la vida social, incluyendo, por supuesto, el de las relaciones de trabajo. Lógicamente, se puede destacar que la proyección del derecho a la protección de datos en el terreno laboral no altera su naturaleza pero, sin embargo, su adecuación sí es determinante a las situaciones generadas en las relaciones de trabajo para convertirlos, así, en verdaderos derechos laborales. Particularmente delicada ya de por sí, esta cuestión lo es aún más si se tiene en cuenta que en nuestro ordenamiento laboral[127] no existe

[126] Según GARCÍA-PERROTE ESCARTÍN, I.; "*el trabajador puede ejercer los derechos fundamentales que como ciudadano tiene reconocidos, no los deja aparcados en la puerta de la fábrica y los recoge cuando sale"* en "Convenio colectivo y contrato de trabajo. Y sobre los derechos constitucionales inespecíficos del trabajador" en ROJO TORRECILLA E.: *Las reformas laborales de 1994 y 1997,* Marcial Pons, 1998, pág. 71.

[127] En este aspecto el Derecho del Trabajo no ha evolucionado todavía lo suficiente como para poder responder a la problemática que puede presentar el avance de las tecnologías informáticas en las entidades que tratan datos personales y en la esfera privada y particular del trabajador. Tan sólo en el art. 4.2 e) del Estatuto de los Trabajadores (Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores publicados en BOE núm. 255 de 24 de octubre) se hace mención al concepto de intimidad del trabajador; *"Al respeto de su intimidad y a la consideración debida a su dignidad,*

todavía, como sería deseable, ninguna norma que reconozca y regule el ejercicio de los derechos fundamentales por los trabajadores, delimitando así su espacio lícito de actuación. El problema queda, de tal forma, librado por lo general a la mediación judicial, con las dificultades e inconvenientes consiguientes[128].

Obviamente, en las relaciones de trabajo se pueden producir revelaciones de datos de los trabajadores que atenten finalmente con la facultad de disposición de su información personal. Estos datos que pueden ser desvelados tienen relación con, entre otros, la afiliación sindical o política, credo religioso, estado de salud, preferencia sexual, etc., cuyo revelación permite al empresario, en un momento dado, ostentar así una posición de privilegio al conocer esta información y poder utilizarla en perjuicio del trabajador. Por este motivo, el derecho a la protección de datos también se proyecta en las relaciones de trabajo, sobre todo como consecuencia de la falta de respuesta de la normativa laboral ante las supuestas amenazas al derecho a la protección de datos de los trabajadores, por lo que será necesario acudir, al igual que ocurriría con cualquier ciudadano, a los mecanismos de defensa establecidos en la normativa sobre protección de datos[129].

Por ejemplo, dentro del ámbito empresarial, si el empresario utiliza dispositivos electrónicos para controlar la productividad o la forma de trabajar de sus empleados y, mediante esos medios, graba esa información para almacenarla en un fichero, se podría atentar contra el derecho a la protección de datos. En estos casos no puede alegarse que se trata de hacer uso de las facultades concedidas por el art. 18 y 20.2 del ET[130], ya que la medida puede

---

comprendida la protección frente al acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual, y frente al acoso sexual y al acoso por razón de sexo".

[128] En este sentido SANGUINETI RAYMOND, W., "Derechos fundamentales del trabajador y poderes empresariales", *Relaciones laborales* núm. 21, 2012, pág.17; DE VICENTE PACHÉS, F: *El derecho del trabajador al respeto de su intimidad*, CES, 1998, pp. 41-43.

[129] PROSSER, W.L.: "Privacy", *California Law Review*, núm. 48, 1960, pp. 366 y ss.; WESTIN, A.F.: *Privacy and Freedom,* Atheneum, Nueva York, 1970, p. 337; MURILLO DE LA CUEVA, P.L: *El derecho a la…*, op. cit., pág. 108.

[130] Art. 18 del ET: *"Solo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del*

llegar a ser desproporcionada si, efectivamente, el trabajador es desconocedor de las posibles grabaciones que se le pueden realizar en el centro de trabajo. Estos preceptos del ET pueden interpretarse de forma flexible, reflexionando sobre su alcance relacionado con la protección de la información personal de los trabajadores si con esos datos se descubren algunas intimidades del trabajador cuyo conocimiento no es necesario para el desarrollo de la relación laboral. Aun así, estos art.s no solucionan los posibles conflictos que se pueden plantear por el ejercicio de los derechos fundamentales en las relaciones de trabajo, por lo que es ineludible acudir a normas ajenas al ámbito laboral para intentar proteger estos derechos pues el ET carece de un tratamiento enfocado a la protección de los derechos fundamentales[131].

Por este motivo, la doctrina científica ha acogido la vigencia de los derechos fundamentales en la relación laboral acuñando el término de derechos fundamentales inespecíficos en relación con aquellos derechos que se atribuyen con carácter general a cualquier ciudadano, pero ejercitados en el seno de una relación laboral por personas que al mismo tiempo son trabajadores, convirtiéndose, de esta forma, en derechos laborales por razón del sujeto y de la naturaleza de la relación jurídica[132]. Esto es lo que ocurre

---

trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible". Art. 20.2 del ET: *"En el cumplimiento de la obligación de trabajar asumida en el contrato, el trabajador debe al empresario la diligencia y la colaboración en el trabajo que marquen las disposiciones legales, los convenios colectivos y las órdenes o instrucciones adoptadas por aquel en el ejercicio regular de sus facultades de dirección y, en su defecto, por los usos y costumbres. En cualquier caso, el trabajador y el empresario se someterán en sus prestaciones recíprocas a las exigencias de la buena fe".*

[131] A pesar de esta situación, la OIT ha dado su punto de vista a favor de la redacción de un conjunto normativo que englobe la protección de datos en el panorama laboral: "*Si bien varias leyes nacionales y normas internacionales han establecido procedimientos de carácter obligatorio para el tratamiento de datos personales, existe la necesidad deperfeccionar las disposiciones específicamente dirigidas al uso de los datos personales de los trabajadores*, en OIT: "Protección de datos personales de los trabajadores" en *Repertorio de Recomendaciones prácticas de la OIT*, Ginebra, 1997, pág. 5.

[132] PALOMEQUE LÓPEZ, M. C.: "Derechos fundamentales generales y relación laboral: los derechos laborales inespecíficos" en VV.AA*: El modelo social en la Constitución Española 1978*, Ministerio de Trabajo e inmigración, Subdirección General de Publicaciones, 2003, pp. 229-230; RODRÍGUEZ-SAÑUDO GUTIÉRREZ, F. Y ELORZA GUERRERO, F.: "Derechos fundamentales laborales inespecíficos", en CASTIÑEIRA FERNÁNDEZ, J. (coord.): *El derecho del trabajo y de la Seguridad Social en el año 2002: puntos críticos*, CARL, Mergablum, 2003. pp. 93-94; GOÑI SEÍN, J.L.: Los derechos fundamentales inespecíficos en la relación laboral individual: ¿necesidad de una reformulación?, en VV.AA.: *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social,* XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, Cinca, 2014, pp. 20-22.

con el derecho a la protección de datos, pues es un derecho global que también tiene que respetarse por las entidades encargadas de gestionar datos de los trabajadores.

Para modular el ejercicio de este derecho fundamental inespecífico, respetando las facultades del empresario como organizador de su propio centro de trabajo (derecho a la libertad de empresa), habrá que atender al juicio de proporcionalidad[133], pues no se podrán llevar a cabo intromisiones ilegítimas que provoquen la revelación de datos personales de los trabajadores, justificando estas actuaciones en el cumplimiento del art. 20.3 ET[134]. Por tanto, será imprescindible comprobar que se cumplen tres requisitos: que la medida restrictiva del derecho a la protección de datos, sea indispensable para conseguir el objetivo propuesto; que la misma sea necesaria, es decir, que no exista otra más moderada o menos represiva; y que la medida sea equilibrada para la consecución del fin, si con su aplicación se logran más ventajas que inconvenientes para el interés general[135].

---

[133] GARCÍA-PERROTE ESCARTÍN, I. Y MERCADER UGUINA, J.: "Conflicto y ponderación de los derechos fundamentales de contenido laboral" en VV.AA*: El modelo social en la Constitución Española 1978*, Ministerio de Trabajo e inmigración, Subdirección General de Publicaciones, 2003, pp. 257-261; GARCÍA-NÚÑEZ SERRANO, F.: "La regularización sobre protección de datos personales y su incidencia en el ámbito laboral", Aranzadi Social, núm. 5, 2000, pág. 1112; CARRIZOSA PRIETO, E: "Las facultades de vigilancia y control en el centro de trabajo y su incidencia sobre el derecho a la intimidad de los trabajadores" en VV.AA.: *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*, Tirant lo Blanch, 2014, pp. 84-86.

[134] Art. 20.3 del ET: "*El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso".*

[135] Criterios seguidos en las siguientes Sentencias: Sentencia del Tribunal Constitucional 292/1993, de 18 de octubre (RTC 1993\292); *"En este punto debemos declarar que este derecho de control del empresario sólo es admisible desde la perspectiva del delegado como órgano de representación sindical, beneficiaria de determinadas ventajas y prerrogativas que entrañan correlativas cargas y costes para la empresa pero carece de fundamento si el delegado se configura como simple instancia organizativa del sindicato -STC 84/1989-. Por consiguiente, no existe inconveniente en reconocer que el empresario puede recabar de la sección sindical o del delegado aquellos datos que precise para comprobar la legitimidad de su creación y elección, pero este poder de control o comprobación encuentra un límite insuperable en los derechos fundamentales del trabajador, que no pueden ser vulnerados por el empresario, obligado a respetarlos, como lo están los propios órganos sindicales".* Sentencia del Tribunal Constitucional 186/2000, de 10 de julio (RTC 2000\186): "*En efecto, de conformidad con la doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan, basta con recordar que –como sintetizan las SSTC 66/1995, de 8 de mayo [RTC 1995, 66] , F. 5; 55/1996, de 28 de marzo [*

Por ello, cuando de relaciones entre sujetos privados se trata, el principal límite al ejercicio de derechos fundamentales debe ser la existencia de otros derechos constitucionales en juego, de manera que el ejercicio de unos derechos no anule o impida el ejercicio de otros y que, por tanto, sólo se admita la limitación de un derecho fundamental en la medida en que es imprescindible para la existencia y ejercicio de otros derechos constitucionales. De modo que la consecución del deseado equilibrio entre los derechos requiere inexorablemente el juicio de ponderación o proporcionalidad entre los derechos que entran en colisión[136].

No obstante, no hay que olvidar que, el empresario también podrá limitar el ejercicio de este derecho fundamental inespecífico, argumentando una posible transgresión del principio de buena fe[137] en la propia dinámica del contrato de trabajo efectuada por el trabajador[138]. Por ejemplo, la negativa de un trabajador a dar su nombre cuando un cliente se lo pide puede ser una acción desproporcionada y que va en contra de lo establecido en el contrato de trabajo o, más bien, en el código de conducta empresarial[139] el cual ha previsto

RTC 1996, 55] , F. 6, 7, 8 y 9; 207/1996, de 16 de diciembre, F. 4 e), y 37/1998, de 17 de febrero [RTC 1998, 37] , F. 8– para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)"; Sentencia 98/2000 de 10 de abril del Tribunal Constitucional (RTC 2000, 98).

[136] SEPÚLVEDA GÓMEZ, M.: "Los derechos fundamentales inespecíficos a la intimidad y al secreto de las comunicaciones y el uso del correo electrónico en la relación laboral. Límites y contra límites", *Temas Laborales: Revista Andaluza de trabajo y bienestar social*, núm. 122, 2013, pág. 210.

[137] Sobre esta cuestión véase entre otros: MORENO GARCÍA, A.: "Buena fe y derechos fundamentales en la jurisprudencia del Tribunal Constitucional", *Revista Española de Derecho Constitucional*, núm. 38, 1993, pág. 263 y ss.; MONTOYA MELGAR, A.: *La buena fe en el Derecho del Trabajo*, Tecnos, 2001, pág. 84; GARCÍA VIÑA, J.: *La buena fe en el contrato de trabajo,* CES, 2001, pág. 19 y ss.

[138] El art. 5 a) del ET menciona entre los deberes básicos de los trabajadores el de "*cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad a las reglas de la buena fe"*.

[139] TASCÓN LÓPEZ, R.: "La protección de datos de carácter personal de los trabajadores", *Revista Jurídica de Castilla y León*, núm. 16, 2008, pp. 459-465.

que los trabajadores tengan que dar sus datos identificativos cuando reciben una llamada o en el ticket de compra[140].

Sin embargo, no parece demasiado acertado, como así ha afirmado la doctrina[141], convertir este principio de buena fe como criterio máximo para valorar una correcta actuación de los derechos fundamentales inespecíficos. Es preciso tener en cuenta que la aplicación de este principio vuelve a tratar el problema de la desigualdad jurídica entre empresario y trabajador como sujetos del contrato de trabajo, pues es evidente que el nivel de exigencia de cumplimiento es mayor para el trabajador que para el empresario[142]. Por todo ello, la jurisprudencia también ha querido hacer alguna aportación sobre este tema, en la Sentencia del Tribunal Constitucional 99/1994, de 11 de abril, en la que se considera el componente principal de la jurisprudencia del TC en materia de garantía y ejercicio de los derechos fundamentales inespecíficos[143].

---

[140] Sentencia de la Audiencia Nacional 52/2005, de 27 de mayo (AS 2005\2728): "*La práctica empresarial denunciada se enmarca en el conjunto de las políticas comerciales llevadas a cabo por los distintos sectores productivos, con la finalidad, también aquí invocada por la defensa, de fidelizar a los clientes y de mejorar la atención al público; en este pleito se han aportado numerosos resguardos, tickets o facturas que reflejan dicha actuación por parte de otras cadenas comerciales y del sector hostelero, y, aunque no reconocidos por los demandantes, es un hecho notorio la existencia de tales prácticas consistentes en priorizar la identificación del personal en contacto con el público con objeto de potenciar la humanización de la relación comercial… Estaríamos ante un supuesto de limitación, y adecuada proporción, a la finalidad que justifica la adopción de la medida, con cobertura en el art. 20 del Estatuto de los Trabajadores (RCL 1995, 997) y que se asienta en la aceptación de una relación jurídica cuyo desarrollo conlleva en el sistema actual este tipo de actuaciones; ya en 1994, lo ponía de relieve una STSJ de Madrid, subrayada por los codemandados, con apoyo en la doctrina del Tribunal Constitucional –STC de 2204.1993 (RA 190/191 [RTC 1993, 142])– cuando excluye del ámbito de la intimidad, constitucionalmente amparado, a «los hechos referidos a las relaciones sociales y profesionales en que se desarrolla la actividad laboral, que están más allá del ámbito del espacio de intimidad personal y familiar sustraído a intromisiones extrañas por formar parte del ámbito de la vida privada".*

[141] VALDÉS DAL-RE, F.: "Poderes del empresario y derechos de la persona del trabajador", en APARICIO TOVAR, J. Y BAYLOS GRAU, A. (coord.): *Autoridad y democracia en la empresa*, Trotta, Madrid, 1992, pág. 48; FERNÁNDEZ LÓPEZ, M.F.: "Libertad ideológica y prestación de servicios", *Relaciones Laborales*, Tomo II, 1985, pág. 65.

[142] En este sentido, RODRÍGUEZ-SAÑUDO GUTIÉRREZ, F.: "La transgresión de la buena fe contractual como causa de despido" en VV.AA.: *Cuestiones actuales de Derecho del Trabajo. Estudios ofrecidos por los catedráticos españoles de Derecho del Trabajo al profesor Manuel Alonso Olea*, Ministerio de Trabajo y Seguridad Social, 1990, pág. 556, ha apreciado un "*desequilibrio muy pronunciado (...) que en términos reales significa que el deber de comportamiento honesto recae con mucho mayor peso sobre el trabajador*".

[143] RTC 1994\99: "...*la modulación del contrato de trabajo sólo se producirá en la medida estrictamente imprescindible para el legítimo interés empresarial (...) o para el correcto y ordenado desenvolvimiento de la actividad productiva (...) reflejo a su vez de derechos que han recibido su consagración en el texto de nuestra norma fundamental – arts. 38 y 33 CE -*" si bien los requerimientos organizativos "*deben venir especialmente cualificados por razones de necesidad, de tal suerte que se hace preciso acreditar – por parte de quien pretende aquel*

3. EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LAS RELACIONES DE TRABAJO.

Una vez determinada la autonomía del derecho a la protección de datos de carácter personal, es preciso profundizar sobre su aplicación en las relaciones de trabajo pues, aunque es obvio que unas normas de carácter global como son la LOPD y el RDLOPD, no van a dar todas las respuestas a los conflictos que puedan suscitarse en torno al acceso y tratamiento de los datos de carácter personal de los trabajadores en el contexto de la relación de trabajo, es inevitable acudir a ellas, así como a otros instrumentos que se describirán ahora, para poder solucionar las posibles infracciones de este derecho del trabajador .

Es cierto que, cuando se redactó el ET no se pensó en ningún momento que la realidad empresarial, relacionada con la implantación de las nuevas tecnologías, que propician un tratamiento masivo de datos personales al incluirlos en ficheros automatizados, iba a sufrir una transformación tan grande en un espacio de tiempo tan corto, razón por la que puede decirse que la normativa laboral ha quedado obsoleta en este tema. Ninguna prohibición o limitación aparece en el ET respecto de la utilización de los medios de almacenamiento de información personal de los trabajadores, como tampoco exige la existencia de formas de protección para controlar el correcto funcionamiento de estas herramientas de gestión de datos de carácter personal. En todo caso, y puesto que es indudable que el uso de las TICS en la relación de trabajo respecto de los datos de los trabajadores debe ser admitida, también es indiscutible que el derecho de los trabajadores debe quedar, en cuanto derecho fundamental, igualmente protegido, para lo que es necesario adaptar la normativa general a la especificidades de las relación laboral.

Es sabido que las empresas (u otras entidades con competencias en el terreno laboral, entendido en sentido amplio) conocen, inevitablemente, datos

---

efecto – que no es posible de otra forma alcanzar el legítimo objetivo perseguido, porque no existe medio razonable para lograr una adecuación entre el interés del trabajador y el de la organización en que se integra".

personalísimos de los trabajadores (como tales o en su calidad de ciudadanos que se relacionan, a partir de su condición de trabajadores, con determinadas entidades, sean públicas o privadas), los cuales se conservan en ficheros automáticos o manuales. Como consecuencia de la realización de estas tareas, es obvio que se pueden ignorar algunos de los principios[144] que fija la LOPD; por lo que hay que analizar las posibles transgresiones del derecho que pueden producirse a lo largo de la vida laboral del trabajador[145].Por otra parte, la especial incidencia del tratamiento de datos en las relaciones laborales pone de manifiesto las dificultades que presenta el utilizar un régimen jurídico genérico como es la normativa de protección de datos, evidenciando la insuficiencia de esa regulación general para tratar supuestos específicos relacionados con la utilización de datos del trabajador[146].

La Comisión Europea ha intentado, sin éxito[147], aplicar la Directiva 95/46/CE a las vicisitudes que pudieran aparecer en el ámbito laboral, mediante la negociación de acuerdos colectivos que permitieran tratar, de forma más precisa, el incumplimiento de los principios y obligaciones impuestas a todas aquellas entidades que gestionan datos de los trabajadores . Y aunque estas actuaciones adolecen del déficit de su carácter temporal podrían servir para identificar todas las cuestiones problemáticas; de forma que el impulso de acuerdos y convenios entre los interlocutores sociales europeos de los Estados Miembros podría servir para establecer posibles soluciones a las vulneraciones

[144] Principio de consentimiento, adecuación y finalidad, así como de información de los datos de carácter personal.
[145] DEL VALLE, J.M: "El derecho a la intimidad del trabajador durante la relación de trabajo", *Actualidad Laboral*, núm. 39, 1991, pp.485-506; SALAS FRANCO, T: "El derecho a la intimidad del trabajador y a la propia imagen y las nuevas tecnologías de control laboral" en VV.AA: *Trabajo y libertades públicas*, La Ley, 1999, pp. 205-206; GOÑI SEÍN, J.L; "Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos de comunicación y archivo de datos" en *Nuevas Tecnologías de la información y comunicación en el Derecho del Trabajo*, Bomarzo, 2004, pp. 56-57.
[146] VALVERDE ASENCIO, A.J: "El derecho a la protección de datos en la relación laboral" en VV.AA.: *Relaciones Laborales y Nuevas Tecnologías*, la Ley, 2005, pp.347-351.
[147] La Comisión Europea propuso en la Comunicación de su Agenda Social una iniciativa para la protección de datos de los trabajadores: "*No obstante, las TIC también ofrecen inmensas posibilidades para recoger y procesar datos sobre el comportamiento personal del trabajador, sus actividades y características, lo que podría tener implicaciones muy graves en caso de un uso no apropiado de los datos",* en Comisión Europea: Comunicación sobre la dimensión social y del mercado de trabajo de la sociedad de la información, 1997. pp.18-19, disponible en: http://pendientedemigracion.ucm.es/info/seas/estres_lab/informes/Informe.[Consulta 2/02/2015]

que se puedan producir del derecho a la protección de datos de carácter personal en las relaciones de trabajo[148].

Así pues, se presenta una realidad compleja, pues toda esta dimensión tecnológica en la prestación de servicios ha traído una nueva gama de conflictos laborales que necesitan respuestas jurídicas y, puesto que la norma legal no proporciona de forma directa soluciones, cabe atender a lo establecido tanto mediante la política empresarial[149], como, sobre todo, a través del convenio colectivo de la empresa, o incluso del contrato de trabajo. Lo lógico sería que, en el marco de la relación de trabajo, la empresa estableciera unas pautas destinadas a informar a los trabajadores de cómo utilizar los datos de carácter personal que tienen que manejar para realizar sus funciones y, normalmente, estas instrucciones están reflejadas en los denominados códigos de conducta empresarial[150]. Aunque, obviamente, carecen de la fuerza de la norma legal y sólo obligan a las partes firmantes del acuerdo sin establecer condiciones para aquellos tratamientos que pudieran realizar terceros ajenos a esa prestación de trabajo. Por ello, para estos terceros se debería establecer alguna instrucción que les advirtiera sobre cómo utilizar esas informaciones para no incurrir en un posible incumplimiento de la LOPD.

---

[148] VV.AA: "La protección de datos en el contexto laboral" en FARRIOLS I SOLA, A. (COORD.):*La protección de datos de carácter…,* op. cit., pp. 64-65; JEFFERY, M.: "Derecho del trabajo en la sociedad de la información" en VV.AA: *Derecho y nuevas tecnologías,* UOC, 2009, pág. 208.

[149] Sobre los códigos de conducta empresarial: CALVO GALLEGO, F.J.: *Códigos éticos y derechos de los trabajadores: una aproximación a la práctica en las empresas españolas*, Bomarzo, 2008, pp. 23-25; GOÑI SEÍN, J.L.: "Valor jurídico de los códigos de conducta" en GOÑI SEÍN, J.L. (coord.): *Ética empresarial y códigos de conductas*, La ley, 2011, pp. 583-626; MALUQUER DE MOTES I BERNET, C.J.: "Códigos de conducta y buenas prácticas en la gestión de datos personales" en LLÁCER MATACÁS, M.R.: *Protección de datos personales en la sociedad de la información y la vigilancia,* La Ley, 2011, pp.118-133; BAYLOS GRAU, A. Y VALDÉS DE LA VEGA, B.: "El efecto de las nuevas tecnologías en las relaciones colectivas de trabajo" en VV.AA.: *Nuevas Tecnologías de la información y comunicación y Derecho del Trabajo*, Bomarzo, 2004, pp.145-152; VV.AA.: *Las relaciones laborales y la innovación tecnológica en España*, Fundación 1º de mayo, 2005, pp. 170-172; TASCÓN LÓPEZ, R.: "La adopción de códigos tipo en el ámbito laboral para la protección para la protección de datos personales" en GOÑI SEÍN, J.L.: *Ética empresarial y…*, op. cit., pp. 531-572.

[150] Por código de conducta se puede entender la implantación de normas internas que tienden a uniformar los estándares de comportamiento exigidos a todos sus empleados, con independencia del servicio que presten en la empresa.

En cualquier caso, lo que sí es llamativo es que muchas de estas entidades, y más concretamente la empresa privada, no se ocupan de este tema en la negociación de sus convenios colectivos y por este motivo desde instancias sindicales se ha sugerido que se aprueben en el seno de la empresa códigos de conducta[151] internos que regulen de forma unilateral la utilización de estos mecanismos. Estos códigos de conducta, ajustados a las obligaciones éticas que ha asumido previamente la empresa, están siendo redactados en muchas ocasiones sin tener en cuenta la opinión del trabajador[152]. La obligación de facilitar el conocimiento de estos códigos a los trabajadores la tiene el empresario y con mucho más sentido deben ser conocedores de esta información aquellos trabajadores que colaboren en la gestión de las bases de datos, de forma que ninguno de ellos pueda alegar desconocimiento de las instrucciones de la empresa[153] respecto al tratamiento de datos[154]. El principal

[151] Al hilo de la implantación de códigos de conducta internos en la empresa que establezcan pautas para tratar los datos de carácter personal el RGPD establece que : *"Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas".*

[152] En algún caso aislado se ha ofrecido la posibilidad a los trabajadores de participar en la redacción de estos códigos. Véanse los Principios de actuación del Grupo Telefónica disponible en http://www.telefonica.com/es/abouttelefonica/pdf/NuestrosPrincipiosdeActuacion .pdf [Consulta 20/02/2015]: "*Nuestros Principios de Actuación han sido formulados contando con las opiniones de nuestros grupos de interés, incluyendo empleados, representantes sociales, consumidores, proveedores, comunidades locales y accionistas".* Código ético de Red Eléctrica disponible en http://www.ree.es/sites/default/files/03_GOBIERNO_CORPORATIVO/ Documentos/C: "*Las personas del Grupo y colectivos de los diferentes grupos de interés han sido invitados a participar en la redacción de este Código, a revisar su contenido, a hacer consultas y a aportar comentarios y sugerencias antes de su aprobación".[*Consulta 02/02/2015]

[153] A modo ejemplo, entre otros, el Código de conducta de Inditex, disponible en http://www.inditex.com/documents/10279/88163/Codigo-de-conducta-y-practicas- responsables .pdf/ [Consulta 06/02/2015], establece que: "*Todos los empleados están obligados a actuar, en sus relaciones laborales con otros empleados, conforme a criterios de respeto, dignidad y justicia, teniendo en cuenta la diferente sensibilidad cultural de cada persona y no permitiendo ninguna forma de violencia, acoso o abuso en el trabajo, ni discriminaciones por razón de raza, religión, edad, nacionalidad, género o cualquier otra condición personal o social ajena a sus condiciones de mérito y capacidad, con especial consideración hacia la atención y la integración laboral de las personas con discapacidad o minusvalías".* Código de conducta del BBVA, disponible en http://www.bbva.com/TLBB/fbinesp/codigo_conducta_bbva_nuevo.pdf [Consulta 06/02/2015]: "*Con independencia de las responsabilidades específicamente asignadas a determinadas áreas del Grupo en materia de seguridad de la información y de protección de datos de carácter personal, los empleados que, por razón de su cargo o de su actividad profesional, dispongan o tengan acceso a este tipo de datos, son responsables de su custodia y apropiado uso. Cumplir con estas responsabilidades requiere: Conocer y observar las normas y procedimientos internos que resulten de aplicación en materia de seguridad de la información y de protección de datos de carácter personal; Aplicar medidas adecuadas para evitar el acceso indebido a tal información".* Política de privacidad de UNIQUE INTERIM S.A.

problema que plantean estas pautas de actuación es que son meros principios para la mejor utilización, en este caso, de los datos de los trabajadores, pero no tienen eficacia o rango de norma legal.

Es evidente que también la jurisprudencia ha intervenido para poder dar solución a la carencia de regulación sobre la protección de datos en los centros de trabajo, al hilo del planteamiento de conflictos en torno a supuestos de posible vulneración de la protección de datos del trabajador. Un ejemplo de ello es la Sentencia, de 8 de marzo de 2002, de la Audiencia Nacional[155] en la que se establece que la utilización de los datos de trabajadores debe ser compatible con la finalidad establecida para la recogida de los mismos,

(ETT); "*Le informamos de que los datos personales facilitados, serán objeto de tratamiento automatizado en los ficheros de UNIQUE INTERIM ETT, S.A. (en adelante UNIQUE) con la finalidad de atender sus preguntas planteadas. Sus datos no serán cedidos a terceras empresas. Salvo que usted manifieste su oposición, consiente expresamente que sus datos sean utilizados para contactar y remitirle información promocional sobre nuestros servicios que puedan resultar de su interés, por cualquier medio, incluido el correo electrónico. En el supuesto de producirse alguna modificación de sus datos, le rogamos nos lo comunique debidamente por escrito. De acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), si lo desea puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición que le asisten, mediante escrito dirigido a UNIQUE en la siguiente dirección….Madrid*." Política de Privacidad de Accenture España**;** *"El objetivo básico del sitio web de Accenture es ser un recurso dinámico y una herramienta que te ayude a conocer mejor Accenture. Queremos que te sientas seguro cuando accedas a nuestro sitio web, y por eso nos comprometemos a preservar tu privacidad siempre que nos visites. Esta política (junto con nuestras condiciones de uso y los avisos sobre privacidad de datos) explica cómo utiliza Accenture los datos personales que podamos recopilar en este sitio web y qué es lo que hace para protegerlos. Al utilizar nuestro sitio web, estás dando tu consentimiento para que Accenture emplee tus datos tal como se explica a continuación. Cualquier cambio que podamos introducir en nuestra política de privacidad en el futuro aparecerá publicado en esta página".*

[154] Los códigos de conducta se han realizado siguiendo el modelo de la Unión Network International, organización sindical creada el 1 de enero de 2000.

[155] JUR\2002\143289: "*En cuanto a si los datos fueron o no usados para finalidad distinta de aquella para la que fueron recogidos, resulta que Caja Cantabria cedió a Vox Pública datos del fichero de "gestión de personal" para realizar un proyecto de investigación sobre niveles de comunicación existentes en la entidad, por medio de un cuestionario que ella misma aprobó y que incluía preguntas sobre el Estado de salud y la ideología de los trabajadores. Puesto que tanto en la LO 5/1992 como en la LO 15/1999 los datos relativos a la ideología y a la salud de los afectados son datos especialmente protegidos, protección que se manifiesta en el procedimiento para recabar los mismos, en el presente caso, puede afirmarse que los datos relativos a personas identificables (o determinables) se han usado para finalidad distinta, como es la de recabar datos sobre ideología y salud al margen de las exigencias que las normas de protección de datos prevén para los que califica como especialmente protegidos. Resulta evidente que los titulares de los datos incluidos en el fichero de gestión de personal desconocían que tales datos personales iban a ser utilizados para la realización de una encuesta en la que les iban a realizar preguntas sobre su salud laboral o sobre su intención de voto y ello impide cambiar la finalidad en su utilización. Sin que tampoco pueda apreciarse la compatibilidad (en la finalidad) a los efectos del art. 4.2 de la LO 15/1999 puesto que las exigencias específicas de la misma Ley Orgánica para recabar tales datos suponen una clara frontera que impide apreciar tal compatibilidad".*

haciendo extensible esta problemática, establecida en la LOPD[156], al ámbito laboral. Por otra parte, se puede apreciar cómo también la jurisprudencia ha tratado el principio del consentimiento en el tratamiento de datos en conexión con las relaciones laborales, siendo prueba de ello la Sentencia de del Tribunal Superior de Justicia de Asturias, de 6 de febrero de 2009[157].

Por todo ello, es necesario adaptar la legislación existente relativa a la protección de datos a las situaciones que se puedan generar en el entorno laboral. Como ha quedado dicho en las líneas anteriores, el trabajador puede solicitar el amparo de la LOPD y el RDLOPD cuando vea peligrar su información personal, razón por la que es necesario hacer un acercamiento descriptivo a lo contenido en estas normas, para, en un momento posterior, trasladar las conclusiones a las relaciones de trabajo[158].

---

[156] La LOPD establece, en su art. 4, el principio de calidad de los datos que tiene como función preservar que los datos sean tratados conforme a la finalidad inicial que propició su recogida. Por ello, en el apartado relativo a los principios de la protección de datos se establecerá el contenido de este principio, así como su proyección a las relaciones de trabajo.

[157] AS 2009\1142*: "la entidad impugnante que el consentimiento exigido para la comunicación de datos cuenta con sus propias excepciones en el mismo precepto legal que se denuncia como infringido, en concreto el Art. 11.2.c) de la LOPD determina que el consentimiento del interesado no será exigible cuando el tratamiento "responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros", en cuyo caso, "la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique", lo que al presente sucede, una vez que la demandada se encuentra incluida en el campo de aplicación del convenio colectivo de la Construcción y, en virtud de las obligaciones dimanantes del referido convenio colectivo y con la finalidad de poder dispensar los servicios asistenciales que allí se pactan, la demandada se halla obligada a abonar a la FLC las cuotas correspondientes a sus trabajadores y, por tanto, la cesión de datos por la Tesorería General de la Seguridad Social, en cuanto no afecta a datos sensibles como pudieran ser la ideología, el origen racial, la salud, la vida sexual etc. sino a los imprescindibles para cumplir con aquella finalidad, ha de ser considerada como legitima. En cualquier caso, sigue diciendo la impugnante, el consentimiento de los interesados no es necesario cuando, como es el caso, se refiere a las partes de un contrato laboral, y estos son necesarios para su mantenimiento y cumplimiento, tal como se dispone el Art. 6.2 de la LOPD y el propio hecho de que sea la Tesorería General de la Seguridad Social quien ha facilitado los datos pone de relieve la legalidad de la emisión de los documentos impugnados…Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos*."

[158] FERNÁNDEZ DOMÍNGUEZ, J.J. Y RODRÍGUEZ ESCANCIANO, S.: *Utilización y control de datos laborales automatizados*, Agencia de Protección de Datos, 1997, pp. 167-176; VV.AA; *Nuevas tecnologías y relaciones laborales,* Aranzadi, 2002, pp. 31-41; THIBAULT ARANDA, J; "*El Derecho*

3.1. Ámbito de aplicación de la normativa sobre protección de datos y su afectación a las relaciones laborales.

Atendiendo a lo establecido en la Directiva 95/46/CE, la LOPD mejora, respecto de la LORTAD, el ámbito de aplicación del tratamiento de datos de carácter personal, incluyendo como novedad que no sólo se va a referir a los ficheros automatizados, sino que también se extiende la protección a los datos insertos en cualquier tipo de soporte[159]. A pesar del ahorro de costes que supone para el mundo laboral la informatización de los datos de carácter personal de trabajadores, la aclaración contenida en la LOPD sobre la extensión de la protección a los ficheros no automatizados se hacía necesaria pues, en el momento en el que se implantó la LOPD, aún existía, y todavía existe, gran parte de documentación almacenada en papel.

Ahora bien, esta ampliación del ámbito de aplicación puede generar problemas interpretativos ya que el art. 2 de la LOPD no transcribe exactamente lo establecido en el art. 3.1 de la Directiva 95/46/CE[160], en el que se menciona que los datos debían pertenecer a un fichero, es decir, limita el ámbito de aplicación a aquellos datos que estén almacenados en un fichero y no en cualquier soporte físico como establece la LOPD. Esta falta de precisión puede justificarse en la voluntad del legislador español de establecer una protección más amplia que la dada en la norma comunitaria en orden a incluir, en el ámbito de aplicación, toda clase de tratamientos de datos sin atender a una posible sistematización de los mismos.

No obstante, aunque la LOPD no lo establezca de forma concreta en su art. 2, es obvio que el ámbito de aplicación se refiere a los datos que estén

---

Español" en VV.AA *Tecnología Informática y Privacidad de los Trabajadores,* Aranzadi, 2003, pp. 75-77.

[159] Art. 2.1. de la LOPD: "*La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado".*

[160] Art. 3.1 de la Directiva 95/46/CE: "*Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".*

almacenados en ficheros[161], pues las definiciones de fichero y tratamiento establecidas en el art. 3 de la LOPD delimitan definitivamente el tema. También, es evidente que estos dos conceptos -tratamiento y fichero- están estrechamente relacionados ya que no parece tener mucho sentido el almacenamiento de datos si posteriormente no existe un tratamiento de los mismos, teniendo en cuenta que se considera tratamiento de datos, también, su simple acumulación en un fichero[162].

Ante esa situación y en caso de duda acerca de si un tratamiento de datos está incluido o no en el ámbito de protección de la LOPD, los Tribunales han resuelto teniendo en cuenta lo establecido en la Directiva 95/46/CE[163], es decir que, según la jurisprudencia, conformarían el ámbito de protección de la LOPD los datos que estuvieran almacenados en un fichero, criterio importante

[161] En la Memoria de la Agencia Española Protección de Datos, 2001 se afirma con rotundidad que: *De otro lado, y aun cuando nos hallemos ante un supuesto en que existan datos de carácter personal, será necesario que dichos datos se encuentren incorporados a un fichero, definido como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso", por el art. 3 b) de la Ley. Ello supone que en el supuesto de que las imágenes no sean objeto de una organización sistemática, con arreglo a criterios que permitan la búsqueda de las mismas a partir de los datos personales de una determinada persona, el archivo en que se contuvieran las cintas de vídeo referidas a dichas personas no será considerado fichero a los efectos de la Ley.* De esta forma soluciona la AEPD la disyuntiva creada a raíz de la falta de precisión del art. 2 de la LOPD cuando habla de soporte físico, estableciendo que ese término está vinculada con la definición dada en la LOPD de fichero.

[162] Sobre este asunto vid., SERRANO PÉREZ, M.M.: *El derecho fundamental...,* op. cit., pp. 284-285.

[163] La Audiencia Nacional, en su Sentencia de 16 de febrero de 2006 (JUR 2006\119381), pretende dilucidar si la actuación realizada por los representantes sindicales entregando el listado de firmas recabadas entre los trabajadores constituye un tratamiento de datos: "*La ley Orgánica 15/1999, por su parte, describe en su art. 2 su ámbito de aplicación mediante una descripción general positiva más genérica que la de la Directiva: será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Es claro para este Tribunal que registro en soporte físico equivale a fichero en los términos de la ley. Basta la lectura completa de este art. 2 y su comparación con el art. 3 de la Directiva del que trae causa, y que sirve para interpretarlo, para llegar a esa conclusión. Pues bien, para que una actuación manual sobre datos personales (recogida, grabación, conservación, elaboración, modificación, bloqueo...) tenga la consideración de "tratamiento de datos personales" sujeto al sistema de protección de la Ley Orgánica 15/1999 es necesario que dichos datos estén contenidos o destinados a ser incluidos en un fichero, esto es, en un conjunto estructurado u organizados de datos con arreglo a criterios determinados. Si no es así, el tratamiento manual de datos personales quedará fuera del ámbito de aplicación de la ley, no será un "tratamiento de datos personales" según el concepto normativo que la ley proporciona. En realidad la existencia del "fichero" en el sentido legal es siempre precisa para que un tratamiento de datos personales esté sujeto al sistema de protección de la ley. En los casos de tratamiento automatizado de datos -siempre sometidos a la ley- es difícil imaginar la inexistencia de un fichero (aunque no se exija expresamente) puesto que los datos que se tratan mediante sistemas automatizados lo son siempre bajo unos criterios de estructura u organización previa".*

para tenerlo en cuenta en cualquier utilización de datos, pues deja entrever que sólo se puede hablar de tratamiento si esa información está contenida en un fichero.

En cuanto a los sujetos objetos de protección, al igual que pasaba en la LORTAD, en la LOPD no se protege la información vinculada a las personas jurídicas[164]. Por tanto, las empresas no gozan de ninguna de las garantías previstas en la LOPD y lo mismo ocurrirá con aquellos profesionales que ejerzan su actividad bajo la forma de sociedad[165]. Lo que se protege son los datos que permiten identificar a una persona física, en nuestro caso a un trabajador, tal y como establece el citado art. 3. a) de la LOPD. Este concepto es también aplicable a la gestión de los recursos humanos ya que, según la definición de la LOPD, en esta actividad se utilizan y tratan datos que se consideran de carácter personal[166].

Esta exclusión de protección de la información de las personas jurídicas se instauró en la LOPD para seguir lo regulado en la Directiva 95/46/CE[167]. Sin embargo, a pesar de lo establecido en la norma comunitaria, ésta no pretende prohibir que en las legislaciones nacionales de los países europeos se pueda contemplar esta protección[168]. Es curioso cómo, en la normativa sobre

[164] Art. 2.2. del RDLOPD: "*Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales".*

[165] Art. 1 de la LOPD: "*La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar",* en relación con el Art. 3.e) de la LOPD: *Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente art..*

[166] Datos que se recogen en actividades relacionadas con recursos humanos en la empresa; datos identificativos, académicos, profesionales (CV), económicos, familiares, formativos, sindicales, de salud, de absentismo laboral, de vacaciones, grabaciones de voz, imagen (video vigilancia) etc.

[167]Considerando 24 de la Directiva 95/46/CE: "*Considerando que las legislaciones relativas a la protección de las personas jurídicas respecto del tratamiento de los datos que las conciernan no son objeto de la presente Directiva".*

[168] A modo de ejemplo, la legislación austriaca sobre protección de datos (Federal Act concerning the Protection of Personal Data (DSG 2000) disponible en: http://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.pdf [Consulta 05/ 02/2015] admite la protección de datos a las personas jurídicas siempre que no sea la encargada de gestionar los datos y cuya información se esté utilizando: Art.4: *"Data Subject : any natural or legal person or group of natural persons not identical with the controller, whose*

protección de datos, esta exclusión de las personas jurídicas no está recogida de forma expresa, aunque se puede deducir del análisis del contenido del art. 3 e) de la LOPD cuando establece el concepto de afectado o interesado[169], no incluyéndose a las personas jurídicas.

Sin perjuicio de lo anterior, esta carencia de regulación del derecho a la protección de datos de carácter personal de las personas jurídicas provoca una contradicción respecto a la jurisprudencia constitucional, puesto que el Tribunal Constitucional ha establecido que hay derechos fundamentales que tendrán que ser reconocidos y protegidos para las personas jurídicas cuando se produzca su vulneración[170]. También el Tribunal Supremo se ha pronunciado sobre esta excepción del derecho a la protección de datos de las personas jurídicas, concretamente en la Sentencia (Sala de lo Civil) de 21 de mayo de 1997[171] en la que se reconoce para las personas jurídicas el derecho al honor el cual está íntimamente ligado al de protección de datos, pero no lo configura como un derecho al que puedan optar finalmente las personas jurídicas,

---

data are processed". En el Codice in materia di protezione dei dati personale italiano, también se contempla la protección para las personas jurídicas, tal y como establece el art. 4.1. f): *"titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza".*

[169] Art. 3 e) de la LOPD: "*Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente art.".*

[170] Sentencia 139/1995, de 26 de septiembre, del Tribunal Constitucional (RTC 1995/139): "*...Hemos dicho que existe un reconocimiento específico de titularidad de determinados derechos fundamentales respecto de ciertas organizaciones. Hemos dicho, también, que debe existir un reconocimiento de titularidad a las personas jurídicas de derechos fundamentales acordes con los fines para los que la persona natural las ha constituido. En fin, y como corolario de esta construcción jurídica, debe reconocerse otra esfera de protección a las personas morales, asociaciones, entidades o empresas, gracias a los derechos fundamentales que aseguren el cumplimiento de aquellos fines para los que han sido constituidas, garantizando sus condiciones de existencia e identidad*". Véase también Sentencia del Tribunal Constitucional 137/1985, de 17 de octubre (BOE núm. 268, de 8 de noviembre de 1985).

[171] Sentencia del Tribunal Supremo (Sala de lo Civil) de 21 de mayo de 1997 (RJ 1997\4122): "*...según el art. 18, aunque parece que lo acentúa en el derecho a la intimidad, ello no excluye la extensión de su protección y garantía a las personas jurídicas respecto a los ataques injustificados que afecten a un prestigio profesional y social, que conforman integración de su patrimonio moral, con repercusión en el patrimonial, por sus resultados negativos, y así puede traducirse en una pérdida de la confianza de la clientela, de proveedores y concurrentes comerciales o de rechazo o minoración en el mercado de forma general y todo ello como consecuencia de que las personas jurídicas también ostentan derechos de titularidad al honor, con protección constitucional, pues no se puede prescindir totalmente del mismo, en su versión de prestigio y reputación profesional, necesarios para el desarrollo de sus objetivos sociales y cumplimiento de los fines para los que fueron constituidas, con un componente de personas individuales, que siempre resultan identificables y a las que también les afecta, en mayor o menor medida, el desprestigio del ente en el que estén integradas".*

aunque exista de facto relación entre ambos y se puedan herir sensibilidades de las personas físicas que integren esa entidad; proponiendo que, en el caso de que se produjeran vulneraciones contra los datos de esas personas, éstas hicieran la oportuna reclamación por las vías administrativa y judiciales habilitadas para ello[172].

A pesar de la disparidad de opiniones doctrinales[173], de lo que no cabe duda es que la protección que se va a analizar es la de la persona física, en este caso de los trabajadores y que, por tanto, las entidades que gestionan sus datos de carácter personal, concebidas como personas jurídicas, están fuera del ámbito de protección de la LOPD y del RDLOPD[174]. Ahora bien, podría darse el caso de incumplimiento de la normativa sobre protección de datos del trabajador respecto al uso de la información concerniente al encargado de gestionar su información personal, ya sea confidencial o no. Pero estas actuaciones del trabajador, si se dieran, supondrían, como ha reconocido la jurisprudencia, una transgresión de la buena fe contractual[175], no pudiendo responder en estos casos por infracción de la LOPD.

---

[172] SANTOS GARCÍA, D; *Nociones generales de la…,* op. cit., pp. 41-43.

[173] Algunos autores discrepan de esta falta de protección de los datos de las personas jurídicas. Así SÁNCHEZ BRAVO afirma que "*la vulneración de sus datos personales no puede menoscabar su intimidad, al menos en la consideración tradicional de esta, pero si puede afectar a otros intereses dignos de protección como intereses económicos o morales"*, en *La protección del derecho…,* op. cit., pág. 128. En este mismo sentido, PÉREZ LUÑO defiende la idea de que "*a medida que el proceso de datos se proyecta a las empresas, a las instituciones y asociaciones se hace cada vez más evidente la conveniencia de no excluir a las personas jurídicas del régimen de protección que impida o repare los daños causado por utilización indebida de informaciones que le conciernen",* en *Manual de informática y derecho,* Ariel, 1996, pág. 58. Para OROZCO PARDO "*la desprotección de la personas jurídicas puede conllevar que éstas no tengan un sistema de defensa ante los ataques que puedan sufrir por la ejecución de algunas de las conductas prohibidas por la norma",* en "Los derechos de las personas en la LORTAD", *Informática y Derecho*, UNED, núms.6 y 7, 1994, pág. 162.

[174] Así lo ha reconocido la Sentencia de la Audiencia Nacional de 19 de marzo de 2014 (JUR 2014\102121): "*De modo que el hecho de que el apartado sexto del precepto establezca que la recogida y el tratamiento de dichos datos "deberá adecuarse a la normativa vigente en materia de seguridad y protección de datos de carácter personal, en cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre , de Protección de Datos de Carácter Personal", atribuyendo la condición de responsables de sus respectivos ficheros a las distintas Administraciones Públicas intervinientes, no supone que los datos sobre compras de medicamentos realizadas por las oficinas de farmacia gocen de la protección que dispensa la citada Ley Orgánica a los datos personales de las personas físicas, ni altera el ámbito subjetivo y objetivo de aplicación de esta Ley".*

[175] Sentencia de 7 de octubre de 2013 del Tribunal Constitucional (RTC 2013\170): "*...transgresión de la buena fe, en la que, entre otros hechos, le imputaba haber mantenido durante mucho tiempo una conducta de máxima deslealtad por haber proporcionado indebidamente información confidencial de la empresa a personal de otra entidad mercantil, sin*

Sin embargo, se puede presentar alguna situación a través de la cual la información relativa a una persona jurídica, o a sus actividades empresariales, abarque datos concernientes a personas físicas pertenecientes al ámbito de organización de su empresa. Asimismo, si los asuntos de la vida profesional también pueden estar sujetos a la protección de datos, parece cuestionable que la protección únicamente se ofrezca a las personas físicas[176]. Por ejemplo, el hecho de que el domicilio social de una persona jurídica conlleve la identificación de personas físicas que viven en él, como podría ocurrir si un empresario comparte su dirección profesional con la familiar. Habrá que atender, entonces, a las circunstancias para determinar si se puede extender el ámbito de protección a esta personas jurídica, superando de esta forma el criterio implantado en la LOPD y en la Directiva 95/46/CE, pues existen algunas normas europeas como la Carta Europea de Derechos Humanos o la Directiva 2002/58/CE que, o bien por su falta de claridad expositiva (relativa a la no exclusión de forma específica de ese derecho)[177], o por contemplarlo expresamente[178], se aplican también a las personas jurídicas.

---

haber pedido nunca autorización para ello y utilizando en dicha transmisión medios que eran propiedad de la empresa -en concreto, teléfono móvil y correo electrónico-. De manera específica, desde el correo electrónico de la empresa, el demandante había transmitido todos los datos relativos a la previsión de la cosecha de 2007 y 2008 a esa otra entidad, incluyendo extremos especialmente sensibles de cuya importancia era conocedor, por lo que no debían transmitirse en ningún caso a nadie de fuera de la empresa".

[176] En el asunto *Volkerund Markus Schecke y Hartmut Eifert contra Land Hessen*,(STJUE de 9 de noviembre de 2010 (TJCE 2010\334) el TJUE, en relación con la publicación de los datos personales relacionados con los beneficiarios de ayudas agrícolas, sostuvo que: "*las personas jurídicas solo pueden acogerse a la protección de los art.s 7 y 8 de la Carta frente a dicha identificación en la medida en que en la razón social de la persona jurídica identifique a una o varias personas físicas. […E]l respeto del derecho a la vida privada en lo que respecta al tratamiento de los datos de carácter personal, reconocido por los art.s 7 y 8 de la Carta, se aplica a toda información sobre una persona física identificada o identificable […]".*

[177] Art. 8 del CEDH: *"Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan".*

[178] Considerando 12 de la Directiva 2002/58/CE: "*Los abonados de un servicio de comunicaciones electrónicas disponible para el público pueden ser personas físicas o jurídicas. Al complementar la Directiva 95/46/CE, la presente Directiva pretende proteger los derechos fundamentales de las personas físicas y, en particular, su derecho a la intimidad, así como los intereses legítimos de las personas jurídicas. La presente Directiva no supone obligación alguna por parte de los Estados miembros de hacer extensiva la aplicación de la Directiva 95/ 46/CE a la protección de los intereses legítimos de las personas jurídicas, que está garantizada en el marco de la legislación comunitaria y nacional".*

Siguiendo con las exclusiones contenidas en la LOPD, es preciso hacer alusión a lo establecido en el art. 2.2 del RDLOPD, dónde se excluye también de la mencionada protección a los ficheros con datos de personas físicas que presten servicios a personas jurídicas cuando únicamente almacenen datos como el nombre y apellidos, la actividad desarrollada en la empresa, así como la dirección postal o electrónica, teléfono y fax profesionales. Con esta enumeración de datos el legislador pretende advertir que cualquier incorporación de datos adicionales, que no pretenda la identificación del sujeto en la persona jurídica a la que presta los servicios, estará sometida a la normativa sobre protección de datos. En este punto, hay que dejar claro que la utilización de estos datos tiene como objetivo tratarlos como datos de contacto en las actividades propias que genere una relación empresarial o profesional, siendo el dato del sujeto únicamente el medio para lograr esa finalidad.

Si se traslada esta exclusión al tratamiento de datos de los trabajadores, y teniendo en cuenta lo establecido por la AEPD para estos supuestos[179], se puede decir que la protección de datos para los ficheros que contengan datos personales de los trabajadores queda desvirtuada, siempre y cuando esa información tenga como objetivo identificar al trabajador dentro de la empresa, así como la descripción de todo lo relacionado con su actividad profesional[180]. Cierto es que, para una efectiva gestión de personal, además de los datos excluidos, es necesaria la recogida de otros datos que exceden del listado

[179] Según la AEPD: " *Por ello, no se encontrarían excluidos de la Ley los ficheros en los que, por ejemplo, se incluyera el dato del documento nacional de identidad del sujeto, al no ser el mismo necesario para el mantenimiento del contacto empresarial. Igualmente, y por razones obvias, nunca podrá considerarse que se encuentran excluidos de la Ley Orgánica los ficheros del empresario respecto de su propio personal, en que la finalidad no será el mero contacto, sino el ejercicio de las potestades de organización y dirección que a aquél atribuyen las leyes…_ Así sucedería en caso de que el tratamiento responda a relaciones "business to business", de modo que las comunicaciones dirigidas a la empresa, simplemente, incorporen el nombre de la persona como medio de representar gráficamente el destinatario de la misma" en* Informe Jurídico 78/2008 disponible en https://www.agpd.es/portalwebAGPD /canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2008-0078.[Consulta 6/02 /2015].

[180] DEL VAL PUERTO, E.: "Zonas de incertidumbre: ámbito de aplicación" en TRONCOSO REIGADA, A (coord.).:*Transparencia Administrativa y…,* op. cit*.,* pp. 473-474; APARICIO SALOM, J.: *Estudio sobre la protección*…, op. cit., pp. 98-99; PIÑAR MAÑAS, J.L.: "Concepto de dato de carácter personal" en TRONCOSO REIGADA, A.: *Comentario a la Ley Orgánica de protección de Datos*, Thomson-Civitas, 2010, pp.196-198.

expuesto, operando, en este caso, lo contenido en la LOPD en relación con el tratamiento de datos de carácter personal[181].

En cuanto al ámbito de aplicación territorial y como consecuencia del carácter transfronterizo que va adquiriendo los tratamientos de datos de carácter personal, tanto en el acceso al empleo como en el desempeño de la actividad laboral, es conveniente establecer las pautas de protección pertinentes. Si bien, atendiendo a la titularidad del dato personal, se presentan algunos inconvenientes, sobre todo en lo relativo a los datos de ciudadanos que se incorporan al mercado de trabajo español y cuyo país de origen no cuenta con una norma que proteja su información personal. Para dar respuesta a esta cuestión, la AEPD[182] ha establecido que los extranjeros inmigrantes tendrán derecho a la salvaguarda de sus datos, atendiendo al criterio de territorialidad pues se encuentran en territorio español y, por tanto, se consideran también sujetos de protección de la LOPD ya que son personas físicas claramente identificables[183].

Por otra parte, teniendo en cuenta la ubicación del responsable del fichero o tratamiento[184], cuando el tratamiento de datos se realice en territorio

[181] DESDENTADO BONETE, A. Y MUÑOZ RUIZ, A.B.: *Control informático, video vigilancia y protección de datos en el trabajo,* Lex Nova, 2012, pág. 96.
[182] Informe AEPD 39/2009 sobre cesión de datos del padrón municipal referido a inmigrantes, aplicación del art. 11.2. a) LOPD, disponible en https://www.agpd.es/portalwebAGPD /canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2009-0039_Acceso-a-datos-Padr-oo-n-Municipal-por-Polic-ii-a-local-y-otras-Fuerzas-de-Seguridad.pdf. [Consulta 20/ 03/ 2015].
[183] SOLANES, Á. Y CARDONA RUBERT, M.B.: *Protección de Datos Personales y Derechos de los Extranjeros Inmigrantes*, Tirant Lo Blanch, 2005, pp. 31-33; SERRANO PÉREZ, M.M.: El derecho fundamental…, op. cit., pp. 268-276.
[184] Art. 2.1. de la LOPD: "*Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal: a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento. b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público. c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito".* Art. 3.1. del RDLOPD: "*1. Se regirá por el presente reglamento todo tratamiento de datos de carácter personal: a) Cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español. Cuando no resulte de aplicación lo dispuesto en el párrafo anterior, pero exista un encargado del tratamiento ubicado en España, serán de aplicación al mismo las normas contenidas en el título VIII del presente reglamento. b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española, según las normas de Derecho*

español en el marco de actividades de un responsable del fichero español, por ejemplo un empresario, ese procesamiento de datos de trabajadores se regulará por la LOPD y por su RDLOPD. También se prevé la aplicación de la LOPD cuando el responsable del fichero no esté establecido en territorio español pero, sin embargo, le sea de aplicación la normativa española. Cosa distinta ocurre cuando el responsable del fichero no está establecido en el territorio de la UE y utilice para el tratamiento medios ubicados en España; supuesto en el que el responsable tendrá que designar un representante cuyos datos deben inscribirse en el Registro General de Protección de Datos para que los afectados puedan ejercer sus derechos[185].

3.2. Configuración del concepto de dato de carácter personal.

Ya se ha indicado, haciendo una aproximación general al concepto de dato de carácter personal establecido en la LOPD, que la información personal de los trabajadores está considerada dato de carácter personal. Si bien se hace necesario realizar un análisis más profundo de este concepto para poder adaptarlo a las relaciones laborales.

En primer lugar, con la amplitud conceptual determinada por el legislador cuando establece la noción de "*cualquier información"*, se pretende incluir, no solo informaciones objetivas, sino también subjetivas basadas en opiniones, encuestas, evaluaciones etc.; es decir, datos no sólo reveladores de aspectos de la vida privada de la persona, sino también de otros aspectos como, por ejemplo, su trayectoria profesional.

Se puede afirmar que esta interpretación amplia del concepto de dato personal es refrendada por lo establecido en el RDLOPD, calificando también

internacional público. c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito. En este supuesto, el responsable del tratamiento deberá designar un representante establecido en territorio español".

[185] SANTOS GARCÍA, D.: *Nociones generales de la…,* op. cit., pág. 48; PLAZA PENEDÉS, J.: "Aspectos básicos de los derechos fundamentales y la protección de datos de carácter personal en Internet" en VV.AA.: *Derecho y nuevas tecnologías de la información y la comunicación*, Aranzadi, 2013, pp. 1147-1148.

como dato de carácter personal: aquella *información numérica, acústica, gráfica, que permita identificar a una persona*[186], siguiendo el criterio establecido en el art. 33 de la Directiva 95/46/CE[187] pero con la diferencia de que, en la definición de la norma comunitaria, no se califican directamente como dato de carácter personal esas informaciones, advirtiendo que sólo se considerará tratamiento de datos los provenientes de imágenes y sonidos cuando sean necesarios y previo estudio de la Comisión Europea. La AEPD también ha apostado por la calificación de las grabaciones de imágenes de una persona o la dirección de correo electrónico que utilice profesional o personalmente como dato de carácter personal, permitiendo así que tengan cabida en el ámbito de protección de la LOPD aquellos conceptos que han ido surgiendo como consecuencia de la evolución de la informática[188]. A pesar de estas matizaciones, el concepto de dato de carácter personal de la LOPD sigue siendo idéntico al mantenido por la LORTAD[189], por lo que no ha variado la definición y se sigue considerando el mismo en sentido extenso, sin que la normativa actual lo haya matizado para acotar su alcance.

En este sentido, y en lo que a las relaciones de trabajo se refiere, la expresión "*cualquier información"* es demasiado amplia y en ella se pueden englobar muchos supuestos distintos que se generan en el momento de la recogida de información de los trabajadores. Así, se pueden enumerar informaciones que afectan a la configuración de datos de carácter personal en las relaciones laborales tales como; las referencias solicitadas a otras empresas sobre la forma de trabajar de una persona que pueden influir en la contratación del trabajador; la información obtenida por la búsqueda del perfil del futuro trabajador en una red social; los datos obtenidos en las entrevistas de selección y en la realización de test psicotécnicos; los datos necesarios para

[186] Art. 5 f) del RDLOPD: "*Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".*
[187] Art. 33.2. de la Directiva 95/46/CE: "*La Comisión estudiará, en particular, la aplicación de la presente Directiva al tratamiento de datos que consistan en sonidos e imágenes relativos a personas físicas y presentará las propuestas pertinentes que puedan resultar necesarias en función de los avances de la tecnología de la información, y a la luz de los trabajos de la sociedad de la información".*
[188] PLAZA PENEDÉS J: "Aspectos básicos de los derechos…", op. cit., pp. 1138-1142.
[189] Art. 3 de la LORTAD: "*Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables".*

cumplimentar un contrato de trabajo; las imágenes e información biométrica captadas en el centro de trabajo, etc.

Es cierto que, para que se hable de tratamiento de datos de carácter personal, estas informaciones deben ser almacenadas o conservadas, por lo que para que esto se produzca habrá que extraer los datos de la fuente de información (acceso) y tratar o utilizar el dato[190]. Esta acción permite diferenciar el mero acceso a un dato del tratamiento que pueda efectuarse a posteriori. Por ejemplo, la simple recepción de un CV sin que se conserven los datos contenidos en él no sería un tratamiento de datos[191]; pero la extracción de la información y su uso para realizar una selección de personal sí lo sería pues ese CV se incluiría en un fichero estructurado, y como tal, tendría que estar, entonces, sometido a lo dispuesto en la normativa sobre protección de datos. Lo mismo ocurre con la visualización de imágenes del centro de trabajo en las que pueden aparecer trabajadores; sin embargo, si estas imágenes finalmente no están guardadas en un fichero, no son susceptibles de tratamiento; aunque hay sectores jurisprudenciales que admiten la existencia de un tratamiento de

[190] El art.1 de la Instrucción 1/2006, de 8 de noviembre, de la AEPD (BOE núm. 296 de 12 de diciembre de 2006) establece que: *"La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras. El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas. Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados. Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma".*

[191] Sentencia de la Audiencia Nacional, de 18 de diciembre de 2006 (RJCA 2007\99): "*Se aduce en la demanda que no hay evidencias de que en los ficheros de Riusa II, SA, existiera constancia de un currículum vitae o solicitud de trabajo de don Valentín, ni hay constancia de la identidad entre el documento recibido por fax y el currículum aportado con la denuncia, pues ni en el Hotel Papagayo Arena, ni en el Hotel Riu Playa Blanca, ni en sus oficinas de personal, ni en los archivos y ficheros existentes se ha encontrado documento alguno a nombre del denunciante, ni se incorporaron sus datos a los ficheros automatizados, por lo que no puede sostenerse la existencia de un tratamiento de datos, tal como establece la LOPD (RCL 1999, 3058) , ya que sólo hubo una comunicación telefónica con el señor Valentín. Se añade en la demanda que en virtud de lo dispuesto en el art. 43.1 LOPD el régimen sancionador únicamente es aplicable a quienes ostenten la condición de responsables de los ficheros automatizados o encargados del tratamiento, existiendo prohibición expresa de que este régimen sancionador alcance a terceras personas. En definitiva para el actor no existe ninguna actuación antijurídica ya que no se ha realizado un tratamiento de los datos Don Valentín de acuerdo con el art. 3.c) de la LOPD, pues ni puede entenderse por tratamiento la simple llamada telefónica realizada, ni sus datos se incorporaron a fichero alguno de Riusa II".*

datos, aunque no se haya producido la grabación de las imágenes, si ha habido transmisión de las mismas a otro monitor para su visualización, sin que hubiera mediado la información pertinente al titular del dato sobre esa captación y sobre emisión de imágenes[192].

En segundo lugar, todas estas informaciones deben servir para identificar a una persona, es decir, habrá que delimitar el término identificado o identificable como lo que es susceptible de diferenciar a una persona en un determinado grupo o cuando sea posible hacerlo teniendo en cuenta una serie de elementos[193]. A pesar de que se puede diferenciar a un trabajador concreto identificándolo por su apellido o por el cargo que ejerza en la empresa, en ocasiones es necesario poner en común varios datos para certificar que se trata de una persona y no de otra; por ejemplo, si ese trabajador tiene un apellido muy común y este criterio no lo diferencia respecto de otros. Por lo que, si lo que se pretende es distinguir un trabajador del resto de los contratados en una misma empresa, quizás sea necesario adoptar otros criterios diferenciadores o complementarios del nombre y el apellido, como puede ser el referido a la actividad que ese empleado desarrolle en el centro de trabajo.

---

[192] Sentencia de la Audiencia Nacional (Sala de lo Contencioso Administrativo) de 22 de enero de 2014 (JUR 2014\38439): "*Pues bien, el apartado c) del art. 3 de la LOPD define el tratamiento de datos como "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias". La captación de imágenes de personas mediante cámaras de video vigilancia y su trasmisión a un monitor, donde es visionada, aun cuando el sistema se limite a posibilitar su visualización, y no su grabación, mediante la reproducción de la imagen de los individuos, constituye una acto de tratamiento de datos de carácter personal que proporciona información de personas físicas identificables acerca de su imagen personal, lugar en que se encuentran y actividad que desempeñan. Por lo tanto, y conforme reiteradamente viene señalando la Sala, entre otras, SSAN, de 3 de febrero de 2011 (JUR 2011, 77335) , Rec. 85/2010, y de 22 de marzo de 2012 (JUR 2012, 141526), Rec. 807/2010, " la simple recogida de datos (aun independientemente de la grabación o conservación) ya constituye un tratamiento de los datos, de las imágenes", y éstas, como dijimos, son datos de carácter personal".*

[193] Considerando 26 de la Directiva 95/46/CE: *"Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta con arreglo al art. 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado*".

Dentro de los datos de carácter personal existen los conocidos como datos sensibles o especialmente protegidos, los cuales tienen un régimen especial e independiente dentro de la LOPD, al igual que ocurría en la LORTAD. Estas informaciones tienen una protección más reforzada debido a su naturaleza específica y a pertenecer al ámbito más íntimo de la persona. Por este motivo y en lo que aquí interesa, quizás los datos sensibles, definidos en la LOPD que más se pueden tratar en el entorno de trabajo sean los relacionados con la ideología, la salud[194] y la afiliación sindical[195] de los trabajadores. Asimismo, para el tratamiento de los datos médicos, será necesario que se solicite al trabajador su consentimiento expreso, o que una ley lo disponga por razones de interés general. Este mismo consentimiento será también necesario para tratar datos sobre afiliación sindical pero, en este caso, tendrá que prestarse por escrito. Las distintas formas exigidas a la hora de recabar el consentimiento para el tratamiento de estos datos sensibles se presenta como un mecanismo que refuerza la protección de esta información respecto de otras.

El tratamiento de estos datos especiales trasladado al ámbito empresarial supone que el empresario no pueda utilizar los datos de afiliación o ideología, entre otros, para fines incompatibles con los que propiciaron su recogida. Con ello, se pretende controlar que la pertenencia a un sindicato pueda influir de forma negativa en una posible contratación del trabajador si, por ejemplo, el encargado de la selección de personal trata o cede los datos de afiliación sindical del futuro trabajador y el empresario utiliza los mismos para no contratarlo. Lógicamente, esta información no es necesaria para realizar una

[194] Art. 7.3 de la LOPD: *"Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente".*

[195] Art. 7.2 de la LOPD: *"Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado".* Art. 7.2 LORTAD: *"Sólo con consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento automatizado los datos de carácter personal que revelen la ideología, religión y creencias".*

correcta selección de personal, a menos que puedan servir para valorar la aptitud del solicitante de empleo para el puesto de trabajo ofertado, por ejemplo, en el caso de las llamadas empresas ideológicas cuya forma de selección de personal se va a tratar en el siguiente capítulo. Aunque lo habitual es que estas informaciones sensibles relativas a la salud, la ideología o la afiliación no tengan relación con la finalidad empresarial y que tampoco sean pertinentes para lograr una adecuada gestión de personal[196].

Para terminar de enmarcar el concepto de dato de carácter personal es preciso hacer referencia a lo establecido en la normativa sobre protección de datos acerca de los datos disociados, y más concretamente sobre lo que se entiende por procedimiento de disociación. Para ello, hay que acudir, en primer lugar, a la acepción contenida en el art. 3 f) de la LOPD sobre "*tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable*" y a lo establecido en el art. 5.1. e) del RDLOPD, en el que se establece que "*dato disociado será aquél que no permite la identificación de un afectado o interesado*[197]". Este concepto jurídico presupone que la información obtenida no puede asociarse a ninguna persona y, por tanto, no se puede identificar claramente a nadie, por lo que estos datos dejan de ser de carácter personal, pues no cumple los requisitos necesarios para ser considerado como tal[198]. La característica principal de un procedimiento de disociación es la posibilidad de realizar un tratamiento de

[196] GOÑI SEÍN, J.L; "Vulneración de derechos fundamentales…", op. cit., pág. 58.
[197] En la Directiva 95/46/CE también se hacía referencia a este procedimiento de disociación, concretamente, en su Considerando 26: *"Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta con arreglo al art. 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado".*
[198] Para DAVARA FERNÁNDEZ- MARCOS. I.:*"…esa información no se puede asociar bajo ningún concepto a una persona física, esa información deja de cumplir con todos los requisitos necesarios para ser considerada un dato de carácter personal*…" en *Hacia la estandarización de la protección…,* op. cit*.,* pág. 164.

datos personales referido a una persona que no puede ser identificada[199] y, por tanto, fuera del ámbito de protección de la LOPD.

También la jurisprudencia ha querido matizar lo que se debe entender por proceso de disociación, estableciendo que hay supuestos en los que no es imprescindible una coincidencia total entre el dato y la persona concreta, sino que es suficiente que tal identificación se pueda realizar sin esfuerzos desproporcionados[200]. Sin embargo, en otros casos[201], ha concluido que, si

[199] Sobre este aspecto el Grupo del art. 29: *"A los efectos de la Directiva, los «datos anónimos» pueden definirse como cualquier información relativa a una persona física que no permita su identificación por el responsable del tratamiento de los datos o por cualquier otra persona, teniendo en cuenta el conjunto de medios que puedan razonablemente ser utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona. «Datos anonimizados» serán, por lo tanto, los datos anónimos que con anterioridad se referían a una persona identificable, cuya identificación ya no es posible",* en Dictamen 4/2007 disponible en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf [Consulta 22/03/2015], pág. 23.

[200] La Sentencia de la Audiencia Nacional, de 8 de marzo de 2002 (JUR 2002\143289) hace alusión a lo que se puede entender por esfuerzos desproporcionados a la hora de averiguar la identificación de una persona establece que:"...*tal y como se desprende del mencionado art. 3 de la Ley, en sus apartados a) y f) y también del Considerando 26 de la invocada Directiva 95/46/CE que expresamente señala que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado;...Aplicando la anterior doctrina a los registros del fichero que fueron proporcionados por Caja Cantabria a la empresa Vox Pública para realizar la encuesta que ahora se enjuicia, y que son los que figuran en los folios 84 a 97 del Expediente, esta Sala considera que los mismos han de reputarse como auténticos datos de carácter personal, al contener información concerniente a personas físicas identificables o determinables, ya que con la edad, sexo, destino, cargo y teléfono de los trabajadores de Caja Cantabria que figuran en el listado proporcionado es obvio que razonablemente, y sin grandes esfuerzos, es posible la identificación de las personas a las que se refieren los repetidos datos., asociación personal que, en cualquier caso, y contrariamente a lo argumentado en la demanda, pudo ya llevarse a cabo por Caja Cantabria al proporcionar los mismo sin grandes dificultades".*

[201] Sentencia de la Audiencia Nacional de 24 de enero de 2003 (JUR 2006\275817): "*La representación de RECOLETOS COMPAÑÍA EDITORIAL, S.A. cuestiona, de un lado, que las imágenes captadas por la webcam situada en la redacción del diario "Marca" puedan ser consideradas "datos de carácter personal", y, de otra parte, que pueda considerarse como "tratamiento de datos" la trasmisión de aquellas imágenes a través de Internet mediante la sucesión de fotos fijas que cambian cada 15 segundos y que no se conservan en archivo alguno… Puesto que la conducta que motivó la sanción objeto de controversia consiste en haber difundido las mencionadas imágenes sin el consentimiento de los afectados, en relación con este reproche de falta de consentimiento se suscitan dos cuestiones. En primer lugar, si nos encontramos en un supuesto de inexigibilidad del consentimiento, conforme a lo previsto en el art. 11.6 de la Ley Orgánica 15/1999, por haber mediado un "procedimiento de disociación". En segundo lugar, si cabe afirmar que en este caso existió consentimiento, sea éste explícito o manifestado de manera implícita o tácita. Partiendo de la definición legal del "procedimiento de disociación" como todo tratamiento de datos personales (realizado) de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable (art. 3.f/ de la Ley Orgánica 15/1999) no cabe afirmar que se haya aplicado aquí un dispositivo de disgregación o difuminación de las imágenes que llegase a impedir la identificación de las*

existe la disociación y no se ha podido certificar, de forma precisa, la identidad de esa persona, se permite entonces el tratamiento de ese dato sin que sea necesario el consentimiento del interesado, a tenor de lo establecido en el art. 11.6 de la LOPD[202]. En otras ocasiones, se puede hacer un uso de los datos disociados con la finalidad de ocultar información que, en un primer momento, tendría que ser prestada, por ejemplo, cuando una sección sindical empieza a recibir la copia básica de los contratos de trabajo con datos disociados, es decir, tan sólo con alguna información. En este caso, analizado por la jurisprudencia en la Sentencia del TSJ de Madrid de 4 de noviembre de 2011[203], se pretende dilucidar si se atenta contra el derecho a la intimidad por el envío de los datos integrantes del contrato de trabajo a los representantes de los trabajadores en la empresa, concluyendo que no existe la citada vulneración pues esta comunicación es parte integrante del derecho a la libertad sindical y como tal debe hacerse sin ocultar ningún tipo de información.

Evidentemente, el procedimiento de disociación se puede utilizar como mecanismo para eludir el cumplimiento de la LOPD, por lo que habrá que observar cada caso concreto para certificar que efectivamente se trata de datos disociados. En el ámbito laboral se pueden captar datos sin que esta información permita la identificación de una persona determinada de esta forma, si la empresa comunicara solamente aquellos datos relativos, por ejemplo, al número de ventas realizada por cada categoría de trabajadores, no estaría incurriendo en una cesión de datos personales puesto que se trataría de datos disociados mediante los cuales sería imposible precisar la identidad

---

personas, pues -volvemos a reiterarlo- las reproducciones que figuran en el expediente ponen de manifiesto que sí es posible la identificación de determinadas personas."

[202] Art. 11.6 de la LOPD: "*Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores".*

[203] Sentencia del Tribunal Superior de Justicia de Madrid, de 4 de noviembre de 2011 (AS 2011\2581): "*Teniendo en cuenta cuanto antecede, a lo que se añade que hasta junio de 2.009 la Dirección Gerencia del Hospital Universitario de La Princesa, Area 2 de Atención Especializada del SERMAS, vino proporcionando sin el menor reparo, ni dificultad, a la Sección Sindical de la FSP-UGT la documentación que desde el mes siguiente le niega, es decir, la copia básica de los nombramientos del personal estatutario de carácter temporal, lo que dejó de hacer con ocasión de un cambio habido en esa unidad directiva, pasando a entregarle solamente unos listados con datos disociados que, no obstante lo establecido en el art. 33.1 del Estatuto Marco del personal estatutario de los Servicios de Salud (RCL 2003, 2934) , no permite el pertinente control sindical de tales nombramientos temporales, y siendo así, además, que facilitar dichos documentos no puede entenderse lesivo del derecho fundamental a la intimidad del personal contratado bajo este régimen jurídico".*

de los trabajadores que han realizado esas ventas[204]. Ahora bien, esta comunicación de datos podría determinar finalmente la identidad de esos trabajadores si se trata de una empresa pequeña en la que se conoce la actividad que realiza cada empleado pues se puede relacionar esta tarea con la producción habida en ese sector de la empresa y posteriormente con el trabajador que tiene asignada esa ocupación.

3.3. Los principios de la protección de datos de carácter personal.

Es evidente que las entidades encargadas de la gestión de recursos humanos, para realizar políticas adecuadas de protección de datos tanto en el acceso al empleo como durante el desarrollo de la relación laboral, tienen que ajustarse a la legalidad respetando los principios establecidos en la normativa sobre protección de datos. Estos principios se encuentran recogidos en el Título II de la LOPD y en el Título II del RDLOPD, respectivamente y, en consecuencia, son los verdaderos inspiradores de la citada protección.

Como es lógico, es preciso identificar y distinguir los principios de la protección de datos para poder aplicarlos a las relaciones laborales y constatar si la utilización de datos de los trabajadores es acorde con la normativa sobre protección de datos. Con este sentido es por lo que, en este apartado, se justifica la descripción genérica de los mismos, profundizando en el contenido del principio de calidad, información y consentimiento. Aun así, la mayor parte de la doctrina muestra insatisfacción respecto de la aplicación de la LOPD a las relaciones de trabajo, por la dificultad de conectar el régimen genérico de la protección de datos con la dinámica existente en cualquier relación laboral, lo que podría justificar la promulgación de una normativa específica para resolver los problemas que se pueden generar en el centro de trabajo[205].

---

[204] Sobre los datos disociados: FATÁS, J.M. Y GARCÍA SANZ, J.M.: "Comentario al art. 5 del Reglamento de desarrollo de la LO 15/1999, de Protección de Datos de Carácter Personal", en PALOMAR OLMEDA, A (coord.).:*Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (aprobado por RDLOPD, de 21 de diciembre)*, Aranzadi, 2008, pp.125-126; LESMES SERRANO, C. (coord.): *La ley de protección…,* op. cit., pp. 114-115; TRONCOSO REIGADA, A.: *Comentario a la Ley Orgánica…,* op. cit*.,* pp. 253-254.

[205] GUALDA ALCALÁ, F.J.: "La protección de los datos personales en las relaciones laborales" en *Estudios de Doctrina Judicial III*, Bomarzo, 2009, pp. 241-249; VALVERDE ASENCIO, A.J: "El

3.3.1. Principio de calidad de los datos.

El principio de calidad de los datos, regulado en el art. 4 de la LOPD, viene a establecer pautas para que los datos que se soliciten sean adecuados, pertinentes y no excesivos, ajustándose en todo momento a una finalidad determinada[206]. Un primer acercamiento al concepto de calidad de los datos muestra cómo el legislador no ha llegado a precisar, por ejemplo, el significado de *"no excesivo*" cuando hubiera sido más explícito introducir un término que aclarara la prohibición de exceso relacionada con el ámbito y la finalidad ya que lo que se pretende con esta acepción es que se traten los datos de forma adecuada a la finalidad que se pretende, sin que ello suponga la recopilación de más datos de los necesarios para ello. Por tanto, se puede considerar, entonces, como excesivos los datos que son indiferentes o que no aportan nada relevante para el normal desarrollo de las actividades relacionadas con La finalidad del tratamiento[207].

Para cumplir con el principio de calidad[208], el encargado de la gestión de las bases de datos tendrá que concretar la adecuación de los datos a las necesidades íntimamente ligadas a su tratamiento; para lo que es indispensable, antes de la recogida del dato, que quede claro lo que se pretende, es decir, con qué finalidad o para que tipo de actividad se acopia la información (explicitud) y su determinación y legitimidad, razón por la que es imprescindible la conexión entre recogida, tratamiento y finalidad. Por este motivo, no basta con que la finalidad sea legítima, sino que se puede prohibir el tratamiento de datos para finalidades que no estén lo suficientemente claras, es

---

derecho a la protección…, op. cit., pp. 355-357; CARDONA RUBERT, M.B.: *Informática y contrato de trabajo*, Tirant lo Blanch, 1999, pp. 105-107; DEL REY GUANTER, S: "Tratamiento automatizado de datos de carácter personal y contrato de trabajo (Una aproximación a la "intimidad informática" del trabajador" *Relaciones Laborales*, núm. 2, 1993, págs. 537 y ss.

[206] Art. 4.1 de la LOPD; "*Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".*

[207] LESMES SERRANO, C.: *La ley de protección…,* op. cit., pp. 141-144; GARCÍA-NÚÑEZ SERRANO, F.: "La regulación sobre protección de datos personales…", op. cit., pp. 5-6.

[208] Art. 4.2. de la LOPD*: "Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos".*

decir, que sean abstractas o inconcretas y no aclaren el verdadero objetivo de la utilización de los datos. También el RDLOPD ha establecido, de la misma manera que la LOPD, que sólo podrán recogerse datos para finalidades determinadas, legítimas y explícitas[209], por lo que se manifiesta la necesidad de que el destino de los datos sea determinado y que se adapte a lo establecido en el ordenamiento jurídico[210].

En consecuencia, la LOPD obliga a tratar el dato para la finalidad prevista, prohibiendo su tratamiento para aquellas finalidades que no sean compatibles y que no hayan sido concertadas en un momento previo al procesamiento de la información personal. Si bien en la LOPD se posibilita el tratamiento de los datos para cualquier finalidad que no sea contraria a la inicial. Para poder acreditar que se cumple con el criterio de la finalidad en el tratamiento de datos es importante que el objetivo que se pretende con su utilización sea lo suficientemente claro como para llegar a descartar cualquier manejo que pueda ir en contra de lo establecido en la normativa sobre protección de datos[211].

La doctrina científica también ha querido matizar lo que se entiende por finalidad incompatible, planteándose la duda de si pueden utilizarse los datos para finalidades distintas o diferentes, pero compatibles con la inicial[212]. Para

---

[209] Art.8.4 del RDLOPD: "*Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".*

[210] MURILLO DE LA CUEVA, P.L: "Las vicisitudes del Derecho…", op. cit., pp. 523-527; FERNÁNDEZ LÓPEZ, J.M.: "La nueva Ley de Protección de Datos de Carácter Personal de 13 de diciembre de 1999. Su por qué y sus principales novedades", *Actualidad Informática Aranzadi*, núm. 34, 2000, pág. 3; APARICIO SALOM, J.: *Estudio sobre la protección…*, op. cit., pp. 221-222.

[211] Sobre el particular, se recomienda el criterio de finalidades distintas, pues es mucho más clarificador que la imprecisión del término incompatibilidad, el cual, ha tenido que ser precisado en sede jurisprudencial y en este sentido, la Sentencia de la Audiencia Nacional de 14 de junio de 2002 (JUR 2003\49779), delimita el término "incompatible" estableciendo*:. "…una interpretación sistemática del mismo poniendo en relación dicha expresión con el principio de autodeterminación que inspira la ley, pues la interpretación amplia de ese término sin tener en cuenta lo establecido en ese principio lo vaciaría de contenido".*

[212] Entiende LESMES SERRANO, que *si la recogida o entrega de datos se realizó con unos fines determinados cualquier uso o tratamiento posterior que no se realice conforme a las finalidades acordadas previamente y sobre las que el afectado no consintió es incompatible con la finalidad que determinó la entrega* en *La ley de protección*…, op. cit., pág. 147. En contra de este planteamiento, APARICIO SALOM, no prevé la existencia de ninguna equiparación entre los términos incompatibilidad y distinción y establece que *la finalidad que se consiente y que el responsable del tratamiento debe respetar es el tipo de actividad a que se destinarán los datos*,

poder precisar si el objetivo del tratamiento es compatible o no con lo previsto inicialmente, y consentido por el titular del dato, habrá que atender a cada caso concreto y determinar, según lo pretendido por la entidad que se encarga del tratamiento de datos, si efectivamente ese procesamiento de datos está prohibido porque llegue realmente a suponer un uso de la información incompatible con su finalidad inicial[213]. Lo que es evidente es que no se puede utilizar la información recogida para otras finalidades no comprendidas, informadas, ni consentidas por el interesado, las cuales no sean compatibles con la originalmente prevista cuando se recogió el dato, ya que si se diera esta circunstancia se tendría que solicitar de nuevo al titular de la información su consentimiento para tratar el dato de forma distinta.

Ahora bien, lo dicho sobre las finalidades incompatibles en el tratamiento de datos ofrece una interpretación dudosa, también, en el marco de las relaciones laborales. En un principio, el empresario no podrá tratar esos datos para fines que no sean acordes con las meras gestiones de la empresa como, por ejemplo, comunicar datos de trabajadores a terceros que nada tengan que ver con el desarrollo de la actividad laboral del trabajador. Pero es indudable que esta vaguedad del concepto puede acarrear problemas exegéticos que pueden llegar a afectar al derecho a la protección de datos de los trabajadores[214].

---

acuñando la noción de incompatibilidad dependiendo de la actividad que se realice y para la que es necesario el tratamiento de datos, en "La calidad de los datos" en TRONCOSO REIGADA, A. (coord.): *Comentarios a la Ley Orgánica…,* op. cit., pág.329.

[213] Sentencia de la Audiencia Nacional (Sala de lo Contencioso Administrativo) de 24 de junio de 2014 (RJCA 2014\580): *"En definitiva, BANKIA S. A., en su condición de sucesora universal en el negocio bancario de Bancaja, es responsable del tratamiento de datos de carácter personal de los denunciantes con infracción del principio de calidad del dato, previsto en el art. 4.3 en relación con el art. 29.4, ambos de la LOPD (RCL 1999, 3058) , cometiendo, por ello, la infracción tipificada en el art. 44.3.c) LOPD , pues se llevó a cabo el tratamiento de datos de carácter personal inexactos, de forma que no correspondían con veracidad con la situación actual de los denunciantes, comunicándose para su inclusión en los ficheros de solvencia Asnef y Badexcug sus datos, asociados a unas deudas inexistentes y sin practicar los requerimientos previos de pago exigibles, con indicación de que de no producirse el pago podrían ser comunicados a los ficheros de solvencia".*

[214] Según la AEPD: "*De este modo, el tratamiento de los datos llevado a cabo por el empresario para el desarrollo de su relación contractual con el trabajador debería limitarse a aquellos datos recabados del trabajador que resultasen adecuados para el desarrollo de la relación laboral, no pudiendo aplicar los datos obtenidos a otra finalidad distinta de la vinculada al desarrollo de la citada relación."* Vid., Informe Jurídico 78/2005 de la AEPD, disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2005-0078 [Consulta 11/04/2015] e Informe Jurídico 184/2006 de la AEPD,

Por este motivo, la jurisprudencia recoge algunos supuestos en los que se produce la vulneración del principio de calidad en las relaciones laborales, por ser la finalidad del tratamiento de datos incompatible con lo previsto en el momento de la recogida de la información. A modo de ejemplo, merece especial atención la Sentencia de la Audiencia Nacional, de 11 de noviembre de 2004, en la que se usan los datos de los funcionarios de una Diputación Provincial y demás personal a su servicio para elaborar determinadas tarjetas de descuento, si bien el verdadero fin que se persigue con la utilización de los datos de afiliación es el de facilitar el censo de trabajadores para las elecciones[215]. Sin embargo, en otras ocasiones, sí se realizan tratamientos de datos considerados compatibles con el objetivo principal que propició la recogida de los datos, como resuelve la Sentencia de la Audiencia Nacional de 15 de junio de 2005[216], en la que se estima que la utilización de datos de un antiguo empleado de la empresa, para enviar una carta a sus clientes informando de la inexistencia de vinculación laboral de ese trabajador con la empresa, se ha hecho para evitar perjuicios a esa empresa por una posible conducta desleal del ex trabajador basada en la utilización de esa cartera de clientes.

---

disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/calidad/common/pdfs/2006-0184 [Consulta 11/04/2015].

[215] Sentencia de la Audiencia Nacional, de 11 de noviembre de 2004 (JUR 2005\232306): "*En definitiva dicha entidad recurrente trató los datos personales de funcionarios y demás personal a su servicio, extraídos de un fichero automatizado de sus dependencias, y los utilizó para finalidades incompatibles con las que justificaron su recogida, ya que no se trataba de facilitar el censo de funcionarios y los medios personales y materiales para la celebración de las elecciones, sino de elaborar determinadas tarjetas que incluían descuentos y otras ventajas que, ofertadas por Multiópticas, fueron remitidas a dichos funcionarios. Por lo que la Diputación Provincial ha cometido la infracción del art. 4.2 de la LOPD, en cuanto usó los repetidos datos para finalidades incompatibles con aquellas para las que los datos fueron recogidos, y al no haber recabado un nuevo consentimiento, ha de concluirse que concurre el «desvió de finalidad» en el uso de los repetidos datos por parte de tal recurrente".*

[216] Sentencia de la Audiencia Nacional, de 15 de junio de 2005 (JUR 2005\240213): "*Entendemos, contrariamente a lo apreciado por la APD, que puede considerarse que la utilización de los datos personales (nombre y apellidos) de dichos denunciantes, por parte de su antigua empleadora, lo fue para una finalidad derivada, o al menos directamente relacionada de dicha relación laboral. Y ello porque una vez efectivo su cese voluntario en Sistemas de Oficina de Algeciras, ésta trató de evitar los perjuicios que le podía suponer una posible "competencia desleal" de aquellos antiguos trabajadores, al servirse de la cartera de clientes de dicha empleadora, y por en consecuencia puede considerarse "compatible" con dicha relación laborar el enviar una carta a los clientes de la empresa advirtiéndoles del cese en ella de tales trabajadores (Sres. Pablo y Ernesto)".*

No obstante, la LOPD establece una excepción sobre este aspecto pues no considera incompatible el uso posterior de los datos con fines históricos, estadísticos o científicos, cuyo tratamiento con este objetivo no haya sido informado en un primer momento. Esta posibilidad de uso de los datos para realizar estadísticas, entre otros, tiene su repercusión en el ámbito laboral, ya que no será necesario informar al titular del dato ni que este consienta el tratamiento de sus datos para la realización de estadísticas relacionadas con el empleo[217], aunque haya prestado esta información con otros objetivos[218].

Por otra parte, dentro del principio de calidad también se exige la veracidad y exactitud de los datos contenidos en el fichero[219], estableciendo, la LOPD previsiones de cómo actuar en el caso de que la información registrada sea inexacta o incompleta[220]. A pesar de que la norma ha distinguido estos dos preceptos (art. 4.3 y 4.4 LOPD) se puede afirmar que jurídicamente la obligación es una sola pues son dos acciones relacionadas ya que la actualización del dato incluye el hecho de corregir los errores o las inexactitudes que pudieran darse, siendo ambos aspectos necesarios para que tenga efecto lo establecido en el tratamiento de datos. Con estas actuaciones se cumple con la previsión del principio de calidad puesto que, con la verificación de los datos contenidos en el fichero, se mantiene, lógicamente, su calidad.

Con este criterio, en lo que a los trabajadores se refiere, se pretende garantizar y proteger la calidad de la información obrante en las bases de datos de las empresas, dando importancia a la actualización de los datos; por ejemplo, en el ámbito de la intermediación laboral adquiere mayor notoriedad este aspecto pues la inserción en una base de datos de un CV debe

[217] Art. 18 g) de la Ley de Empleo: "*Mantener las bases de datos generadas por los sistemas integrados de información del Sistema Nacional de Empleo y elaborar las estadísticas en materia de empleo, formación y protección por desempleo a nivel estatal".*
[218] APARICIO SALOM, J.: *Estudio sobre la protección*…, op. cit., pp. 226-228.
[219] Art. 4.3 de la LOPD: "*Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado".*
[220] Art. 4.4 de la LOPD: "*Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el art. 16".*

contemplar la posibilidad de que esté pueda sufrir modificaciones, ya que el demandante de empleo ha podido adquirir experiencias formativas o laborales nuevas distintas a las introducidas cuando se dio de alta como solicitante de empleo. En este supuesto, se exige la veracidad y exactitud de los datos como medio para enriquecer el CV y poder ampliar las posibilidades de adquirir un empleo, pudiendo conllevar la inexactitud o falta de certeza de los datos la limitación de acceder a determinadas ofertas de empleo[221].

La cancelación de los datos de carácter personal, forma parte también del principio de calidad y queda recogida en el art. 4.5 LOPD[222]. Entre la cancelación y la finalidad del tratamiento existe una evidente conexión ya que, cuando termina el objetivo para el cual los datos han sido recogidos, es lógico pensar que esos datos ya no son necesarios ni pertinentes para cumplir la finalidad determinada en su recogida, por lo que el responsable del fichero tiene que proceder a cancelarlos o eliminarlos del fichero en dónde estén ubicados. Indudablemente, la finalidad de un fichero se extiende durante un periodo de tiempo concreto, aunque a veces no es fácil precisar su duración pues hay ocasiones en las que la finalidad principal está vinculada a otras necesarias para su cumplimiento[223].

---

[221] MURILLO DE LA CUEVA, P.L.: "Informática y protección de datos personales" en *Estudios sobre la LO 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*, col.43, Cuadernos y Debates, Ed. Centro de Estudios Constitucionales, 1993, pp. 64-68.

[222] Art. 4.5 de la LOPD: "*Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos".* Este principio sigue con las pautas establecidas en el art. 5 e) del Convenio 108, en el que se establece que, si falla la necesidad o pertinencia que propició la relación entre el tratamiento y la finalidad, esos datos serán cancelados.

[223] Por ejemplo, en el ámbito de la Administración Pública, concretamente en el departamento de recaudación ejecutiva de un Ayuntamiento, no se requieren los datos para sólo tramitar un procedimiento de apremio sino que también se necesitan para emitir una certificación acreditativa de la cancelación de la deuda, para la cual no se exige ningún plazo, entendiéndose que podrá realizarse en cualquier momento. (art. 41 Real Decreto 939/2005, de 29 de julio, por el que se aprueba el Reglamento General de Recaudación. BOE núm.210 de 2 de septiembre de 2005).

Esta apreciación legislativa tiene mucho más sentido desde que la informatización de los datos de carácter personal ha hecho incursión en el mundo empresarial pues el uso de la informática puede generar que esos datos queden almacenados y que el titular del dato no sepa de forma fehaciente que se hayan cancelado. La mecanización de las bases de datos permite la memorización de un gran número de ficheros con información y la incertidumbre de no saber la ubicación física de los datos y, lo más importante, si la cancelación es definitiva o permanecen en la memoria interna del ordenador más tiempo del debido[224].

Por otro lado, hay que recordar que otro de los parámetros para el cumplimiento del principio de calidad es la comprobación de que la recogida de datos se haga a través de medios lícitos[225]. A estos efectos, el encargado de la gestión de personal tendrá que utilizar medios que no desvirtúen el derecho a la protección de datos y que capten los datos de forma legítima, informando al trabajador de que esos medios cumplen con las garantías pertinentes para asegurar la información dada. En el mismo sentido, utilizar medios con la única finalidad de descubrir más datos de los necesarios, es un claro ejemplo de uso de medios para obtener datos de manera ilícita[226].

3.3.2. Principio de información.

Este principio, que debe manifestarse en el momento de recogida de los datos informando a su titular sobre el uso o destino que se le va a dar a su información personal o posteriormente si los datos son recabados de otras

[224] SERRANO PÉREZ, M.M: *El derecho fundamental...* op. cit., pp. 435-437.
[225] Art. 4.7 de la LOPD: "*Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos*".
[226] VIZCAÍNO CALDERÓN, V.: *Comentarios a la Ley Orgánica de Protección de Datos*, Civitas, 2000, pp. 91-99; APARICIO SALOM, J.: "La calidad de los datos" en VV.AA*.: Comentario a la Ley Orgánica…,* op. cit., pp. 323-340; DAVARA RODRÍGUEZ, M.A.: "Acerca de los principios del consentimiento y calidad de datos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD)", *Revista técnica especializada en administración local y justicia municipal*, núm. 2, 2009, pp. 256-261; LESMES SERRANO, C (coord.): *La ley de protección…,* op. cit., pp. 148-160; RODRÍGUEZ ESCANCIANO, S.: El derecho a la protección de datos personales de los trabajadores: nuevas perspectivas, Bomarzo, 2009, pp.19-27; SANTOS GARCÍA, D; *Nociones generales de la…,* op. cit., pp. 57-63; AIMO, M.P.: "Tutella della riservatezza e protezione dei dati personali dei lavoratori" en VV.AA.: *Tratato di diritto del lavoro*, vol. IV, tomo II, Padova, CEDAM, 2012, pp. 1776-1778.

fuentes[227]. A su vez, la normativa sobre protección de datos establece que el modo de informar debe ser expreso[228], preciso e inequívoco[229], para que no pueda inducir a confusión y con el objetivo de que el titular del dato conozca no sólo la finalidad del tratamiento de datos, sino también los usos que le va a dar el responsable del tratamiento para conseguirla. De forma que, con carácter general, la información que este responsable debe dar al titular del dato ha de ser lo más amplia posible[230], para que conozca, también, qué personas van a utilizar su información además del responsable del fichero[231].

Este principio, adaptado al ámbito laboral, significa que los trabajadores deben estar informados, en primer lugar, de la existencia de ficheros con sus datos personales y, en segundo lugar, de la finalidad para la que fueron creados esos ficheros. Es obvio que en las relaciones de trabajo el tratamiento de esos datos tiene como finalidad la gestión de los recursos humanos de la empresa y, por tanto, este debiera ser el único objetivo por el que se solicitan los datos de carácter personal. Ahora bien, si realmente se ha respetado el principio de información y se realiza un procesamiento de datos conforme a las

[227] Vid., art. 5.4 de la LOPD.
[228] La LOPD relativiza la exigencia de que la información se otorgue de forma expresa al establecer su art. 5.3, que no será necesario que se dé información de esta manera si el contenido de ella se deduce claramente de la naturaleza de los datos que se van a tratar.
[229] Sobre la prestación de información de forma inequívoca véase: Informe jurídico 340/2010 de la AEPD disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/ informes_ juridicos/deber_informacion/common/pdfs/2010-0340_Cumplimiento-de-la-obligaci-oo-n-de-informaci-oo-n-sobre-tratamiento-de-sus-datos-a-clientes.-Idioma.pdf. [Consulta 04/04/ 2015]
[230] En el art. 13 del RGPD se especifica más detalladamente toda la información que debe conocer el titular del dato acerca del tratamiento que se va a realizar a su información personal. Se indica que el responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda la información de los datos personales que se obtengan de él y que esta información incluya en su caso, información sobre los datos de contacto del delegado en protección de datos. Además, se deberá informar al interesado sobre el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar ese plazo.
[231] Art. 5.1 de la LOPD; "*Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a. De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b. Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c .De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento".*

advertencias dadas a su titular, éste no podrá recriminarle al responsable del tratamiento que sus datos se están utilizando sin que se conozcan sus fines, ya que parece extraño que el interesado haya deba prestar su consentimiento sin conocer a quien se le entregan los datos y con qué objetivo o destino se usan. A su vez, esta información[232] está íntimamente conectada con el principio de calidad[233] justificando esta conexión en la advertencia explícita, al titular del dato, sobre la finalidad del tratamiento trasladando, de esta manera, esa obligación a la persona que va a realizar el tratamiento y conectándola con el cumplimiento del principio de información, ya citado.

El principio de información tiene especial importancia porque se configura como aquel que permite a cualquier ciudadano y también al trabajador, el ejercicio de los derechos de acceso, rectificación, oposición y cancelación[234]. Para ello es necesario conocer la identidad y dirección del responsable del fichero, sin que la utilización de fórmulas genéricas induzca a confusión pudiendo provocar situaciones en las que no se sepa realmente ante qué entidad se tienen que ejercer los derechos citados[235]. Sobre este aspecto se ha pronunciado la Sentencia de la Audiencia Nacional, de 15 de junio de

---

[232] Sobre el principio de información vid., CARDONA RUBERT, M.B.: *Informática y contrato...,* op. cit., pp. 125-127; RUIZ CARRILLO, A: *Los datos de carácter personal*, Bosch, 1999, pp. 76-77; DAVARA RODRÍGUEZ, M.A.A.: "La nueva Ley Orgánica de protección de datos de carácter personal", en VV.AA.: *XIII Encuentro sobre informática y Derecho*, Aranzadi, 2000, pp. 30-31; VIZCAÍNO CALDERÓN, V.: *Comentarios a la Ley Orgánica…* op. cit., pp. 101-111; SANTOS GARCÍA, D; *Nociones generales de la*… op. cit., pp. 63-67; HERRÁN ORTIZ, A.I.: *El derecho a la intimidad en la Nueva Ley Orgánica de protección de datos personales*, Dykinson, 2002, pp. 215-220; CANALES GIL, A.: "Las competencias sancionadoras de la AEPD y el procedimiento sancionador: de nuevo sobre los principios de información y consentimiento" *Revista Jurídica de Castilla y León,* núm.16, 2008, pp.181-182.

[233] Art. 5.1. b) y c) de la LOPD.

[234] Art.5.1 d) y e) LOPD.

[235] Sobre este particular la AEPD ha sancionado una cláusula de información que decía: "*Es posible que si, usted no nos indica lo contrario, comuniquemos sus datos personales a otras empresas asociadas a la Federación Española de Comercio Electrónico y Marketing Directo pertenecientes a sectores financieros, seguros, venta a distancia, editorial , y a ONG asociadas o no a tal Federación."* Vid., Procedimiento Sancionador PS/00014/2006, de 7 de julio, disponible en http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos _sancionadores /ps_2006/common/pdfs/PS-00014-2006_Resolucion-de-fecha-07-07-2006_Art-ii-culo-5-LOPD .pdf [Consulta 07/01/2015] y en el mismo sentido vid., Procedimiento Sancionador PS/00328/2005 de 31 de julio de 2006 en el que se expone: *"Los datos personales que usted nos facilitó serán incluidos en el fichero automatizado de CEAC S.L. para gestionar la relación comercial con usted…Es posible que en un futuro-incluso finalizada la relación comercial-utilicemos sus datos personales para informarles sobre nuestros productos y servicios o que comuniquemos tales datos a las empresas que integran el grupo mercantil Planeta."* En ambos casos no queda determinado de forma clara y concisa quien es el responsable del fichero en las posibles comunicaciones de datos que se puedan realizar desde el fichero automatizado.

2001[236], en la que se muestra el principio de información como uno de los pasos previos al ejercicio de los derechos de acceso, rectificación, oposición y cancelación. Por tanto, el responsable del fichero será el encargado de dar, entre otras, la información relativa al ejercicio de los citados derechos; por lo que, lógicamente, el titular del dato tendrá que conocer con exactitud quien es la entidad que gestiona el fichero, pues frente a ella tiene que ejercitar los citados derechos[237].

Hay ocasiones en las que se utilizan formularios o impresos[238] para recabar información y estos deberán contener las advertencias citadas en el art. 5.1 de la LOPD[239]. Sobre este aspecto cabe mencionar que la inscripción de estas notas en los cuestionarios o formularios habilitados para recoger información personal debe ser claramente legible e inteligible[240], siendo extensivas estas características al supuesto en el que los datos se recojan por Internet. Si esos datos son captados por un operador telefónico, habrá que fortalecer los mecanismos para poder certificar que se le ha dado esa información a su titular[241]. Es obvio que la inserción en los impresos o cuestionarios de recogida de información personal de notas informativas con lo establecido en el art. 5.1 de la LOPD es lo más acertado, y se realiza en beneficio del principio de seguridad jurídica[242], para que de esta forma el

[236] JUR 2001\293673.
[237] LESMES SERRANO, C (coord).: *La ley de protección*…, op.cit., pp. 170-175; CANALES GIL, A.: "Derecho de información en la recogida de datos" en VV.AA.: Comentarios a la Ley Orgánica de Protección…, op. cit., pp. 406-412; ZABIA DE LA MATA, J.: *Protección de datos: Comentarios al Reglamento*, Lex Nova, 2008, pp. 174-176.
[238] En la gestión de recursos humanos es muy común que el trabajador tenga que cumplimentar formularios con preguntas sobre su actividad profesional y con sus datos identificativos. En otro orden de cosas, también existen impresos para recabar datos sobre la salud de los trabajadores previamente a los reconocimientos médicos que puede realizar el empresario, por lo que estos datos sanitarios tendrán que tratarse de forma específica tal y como prevé la normativa sobre protección de datos de carácter personal.
[239] Vid., pp. 63-64.
[240] Art. 5.2 de la LOPD*: "Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior".*
[241] Normalmente, en el caso de llamadas telefónicas que recaben información de un particular o del propio trabajador, se realiza una grabación en la que se le informa de lo citado en el art. 5.1 LOPD, quedando de esta forma cumplida la obligación de información que tiene la entidad que va a ser responsable del fichero de datos de carácter personal.
[242] Art.18 del RDLOPD: "*1.El deber de información al que se refiere el art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado. 2. El responsable del fichero o tratamiento deberá conservar el soporte en el que*

responsable del fichero y del tratamiento puedan probar que han cumplido con su deber de informar[243].

Como se ha comentado, también se puede admitir la práctica de la obligación de informar en un momento posterior a la recogida de información porque ésta haya sido recabada de otras fuentes distintas al interesado. Este pudiera ser el caso de las emergencias sanitarias, pues en esa ocasión el titular del dato no está en condiciones físicas o psíquicas como para recibir información sobre el tratamiento que se le va a dar a sus datos personales. Por este motivo, en el marco de la relación laboral, si se produce algún tipo de accidente de trabajo, es bastante frecuente que esos datos los dé otra persona, que normalmente es el empresario, pues el trabajador no está en condiciones de hacerlo. En estos supuestos, en los que será prioritario atender médicamente al trabajador[244], el legislador ha previsto que se pueda exceptuar el consentimiento para tratar el dato[245]; por lo que no tendría sentido exigir el cumplimiento del deber de información previo a la recogida del dato si tampoco se requiere el consentimiento para el tratamiento.

Cuando los datos no se hayan obtenido de los propios interesados existen excepciones al principio de información, establecidas en la normativa sobre protección de datos, en las que no resulta necesario que éste se ponga

---

conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes original".

[243] CANALES GIL, A.: "Derecho de información en…", op. cit., pp. 414-418; LESMES SERRANO, C (coord).: *La ley de protección*…, op. cit., pp. 176-177.

[244] Esta obligación de informar al trabajador podría suplirse utilizando el medio que mejor se adapte, mediante la inclusión de una cláusula informativa en el informe médico que se le da una vez cumplimentada la asistencia médica, pudiendo, si el trabajador lo estima oportuno, oponerse o cancelar sus datos del fichero creado con su información médica y personal.

[245] Art. 7.2. de la LOPD*: "No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del art. 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".*

en práctica[246]. Estas excepciones al principio de información se producen: cuando exista una norma que permita su tratamiento[247]; cuando la recogida de datos tenga como finalidad realizar estudios estadísticos, históricos o científicos; o cuando el cumplimiento de la obligación de informar resulte imposible o exija un esfuerzo desproporcionado.

Conviene detenerse en la exención relacionada con el hecho de que el responsable del fichero no pueda ejercer su deber de información porque este exija un esfuerzo desproporcionado. En este caso, la normativa prevé que sea la AEPD la que determine la causa que justifique que el cumplimiento de esa obligación no es posible. Hoy día, parece difícil pensar que, precisamente debido a la implantación de la TICS en casi todo los ámbitos, no sea viable comunicar a los interesados la información referida al tratamiento de sus datos, ya que, en cualquier momento y utilizando los medios informáticos, se pueden dar advertencias generales que pueden enviarse a un gran número de personas con el simple hecho de anunciar la información sobre el tratamiento en la web o enviando una leyenda común donde se informe de las pautas a seguir en el tratamiento. No obstante, la indeterminación del precepto puede crear confusión a la hora de verificar el cumplimiento de la normativa sobre protección de datos, pues la única entidad competente para establecer la exoneración del deber de información es o la AEPD[248].

---

[246] Art. 5.5 de la LOPD: "*No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias".*

[247] Por ejemplo, a la hora de confeccionar el censo electoral al amparo de lo establecido en el art. 32 de la Ley 5/1985 de 19 de junio, de régimen Electoral General (BOE núm. 147 de 20 de junio de 1985); "*1.La inscripción en el censo electoral es obligatoria. Además del nombre y los apellidos, único dato necesario para la identificación del elector en el acto de la votación, sin perjuicio de lo dispuesto en el art. 85, se incluirá entre los restantes datos censales el número del Documento Nacional de Identidad. 2. Los Ayuntamientos tramitan de oficio la inscripción de los residentes en su término municipal. 3. Las Oficinas Consulares de Carrera y Secciones Consulares de las Misiones Diplomáticas tramitarán de oficio la inscripción de los españoles residentes en su demarcación en la forma que se disponga reglamentariamente".*

[248] CANALES GIL, A.: "Derecho de información en…", op. cit., pp.421-423; LESMES SERRANO, C (coord).: *La ley de protección*…, op. cit., pp. 183-188.

Ahora bien, pueden darse supuestos en los que la finalidad inicial del fichero se ha modificado y, por consiguiente, sea necesario utilizar el dato de forma distinta a la advertida en la cláusula informativa. La normativa sobre protección de datos no recoge esta peculiaridad, quizás por no haber tenido en cuenta lo establecido en el art. 7 f) de la Directiva 95/46/CE[249], por lo que el responsable del fichero está obligado a volver a informar al titular sobre los nuevos usos que se le van a dar a los datos, con el objetivo de obtener un nuevo consentimiento para tratarlos[250]. Si bien en las empresas de trabajo temporal, capacitadas no sólo para seleccionar trabajadores sino también para cederlos a la empresa que contrata sus servicios, una vez que el solicitante de empleo es contratado, sus datos, además de otros imprescindibles para formalizar el contrato de trabajo, pasan a formar parte de un fichero distinto, pues ya pertenecen a la plantilla de trabajadores de la empresa de trabajo temporal. En este supuesto, habrá que informar a estos trabajadores de la finalidad de ese fichero, ya que el objetivo va a ser distinto y, por tanto, el intermediador laboral tendrá que volver a recabar el consentimiento del titular del dato para que puedan ser utilizados, en este caso para realizar gestiones relativas, entre otras, a su contratación laboral[251].

3.3.3. Principio del consentimiento.

El principio de consentimiento se configura como un principio estrechamente relacionado con el de información[252]. Esto supone que el

[249] Art.7 f) de la Directiva 95/46/CE: "*Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse*… si:*es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del art. 1 de la presente Directiva".*

[250] SOLAR CALVO, M.P.: "La protección de datos en la Unión Europea: análisis y perspectivas de futuro." *Revista Aranzadi Unión Europea*, núm. 2, 2012, pp. 23-35.

[251] Es preciso destacar que, en otros países europeos como es el caso de Portugal, no se dispone que sea necesario volver a pedir el consentimiento sin cambia la finalidad del tratamiento, estableciendo el art. 23.1 c) de la Ley 67/1998, que será la Comisión Portuguesa la encargada de valorar y, en su caso, autorizar el tratamiento de datos basado en el interés legítimo del responsable del fichero: "*Autorizar excepcionalmente a utilização de dados pessoais para finalidades não determinantes da recolha, com respeito pelos princípios definidos no artigo 5º".*

[252] La jurisprudencia también se ha posicionado a favor de esta afirmación, ya que la citada Sentencia 292/2000 de 30 de noviembre del TC (RTC 2000/292) establece que: *"son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso*

consentimiento prestado por cualquier ciudadano para que sus datos sean tratados tendrá que venir precedido de una declaración de voluntad realizada por el responsable del fichero, en la que se exponga, de forma clara y concisa[253], los datos que van a ser objeto de tratamiento y las intenciones que tiene para con ellos, de esta manera, el ciudadano conozca toda la información antes de consentir el procesamiento de sus datos[254].

Otro de los aspectos destacables en lo que a la prestación del consentimiento se refiere, es el momento en el que éste se debe prestar ya que, en la organización sistemática de la LOPD, este principio aparece después de los de calidad e información, por lo que se puede entender que el consentimiento del titular del dato ha de prestarse en un momento posterior a la recogida y antes de que se inicie el tratamiento del dato. Esta afirmación tiene sentido y se justifica en que la propia LOPD tan sólo exige que medie el consentimiento para los supuestos de tratamiento de datos y cesión, pero nada dice sobre la prestación del mismo en la recogida de la información[255]. Quizás la razón por la cual el legislador no fije el momento en el que se debe prestar el consentimiento tiene su justificación en la intención de que, desde el principio

---

de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos".

[253] El RGPD refuerza la prestación del consentimiento por parte de los titulares de los datos instando por una manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen teniendo en cuenta que, cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales (vid., art. 7 del RGPD).

[254] Art. 12.2 del RDLOPD: "*El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes. La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos".*

[255] Sin embargo, HERRÁN ORTIZ advierte que en la LORTAD si se diferenciaban dos consentimientos, uno para la recogida, y otro para el tratamiento posterior, "*consciente de que son operaciones perfectamente diferenciables introduce con acierto la distinción en la exigencia del consentimiento en la fase de recogida y en el posterior tratamiento* en *La violación de la…,* op. cit., pág.255. Se advierte que este criterio diferenciador del consentimiento seguido por la autora, no encuentra su ubicación en la LORTAD ni en la LOPD, pues no se establecen distinciones relativas a los distintos momentos en los que el titular del dato debe prestar el consentimiento; tan sólo, se refiere a la recogida del consentimiento para el tratamiento y cesión, sin ni siquiera tener previsto la prestación del consentimiento para el acceso a los datos de carácter personal.

(recogida del dato), el interesado debe conocer el tratamiento que se le va a dar, y es a partir de ese conocimiento cuando tiene que decidir si consiente o no la utilización de sus datos para los fines establecidos[256].

Por tanto, la aplicación de estos principios está vinculada por un doble motivo: en primer lugar, porque no parece razonable exigir un consentimiento de algo que en realidad no se conoce; y, en segundo lugar, dado que la prestación del consentimiento está condicionada a las advertencias que sobre la utilización de su información personal se le den al titular, se entiende que éste puede alegar incumplimiento del principio de información si dicha información se utiliza para otros fines distintos de los advertidos en el momento de consentir su tratamiento[257].

Dicho esto, una de las razones para la modificación de la LORTAD, fue la forma en la que el afectado tenía que facilitar el consentimiento para el tratamiento de sus datos de carácter personal, pues era un aspecto que se regulaba de forma muy superficial. En la nueva regulación se ha intentado precisar más el concepto de consentimiento, ya que el establecido en el art. 6 de la LORTAD[258] no contenía las características concretas con las que éste tenía que ser otorgado -establecía simplemente que era necesario el consentimiento del afectado- aspecto que la LOPD[259] ha modificado caracterizándolo finalmente como un consentimiento inequívoco[260], explícito y sin reservas, acotando mucho más el término.

Siguiendo el mismo criterio implantado por la LORTAD, la actual normativa sobre protección de datos establece que el consentimiento será

[256] VIZCAÍNO CALDERÓN, M.: *Comentarios a la Ley Orgánica…,* op.cit., pp. 113-115; TRONCOSO REIGADO, A; *La protección de datos personales…,* op. cit., pp.1566-1569; LESMES SERRANO, C.(coord.): *La ley de protección…,* op. cit., pág. 193.
[257] DÍAZ REVORIO, F.J.: "Derecho de información en la recogida de datos. Una perspectiva constitucional" en VV.AA.: *Comentarios a la Ley Orgánica de Protección…,* op. cit., pág. 435.
[258] Art. 6 de la LORTAD: "*El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa".*
[259] Art. 6.1 de la LOPD: *"El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa"*.
[260] Según la Real Academia de la Lengua Española el término inequívoco se define como "*que no admite duda o equivocación."* Por lo que, el consentimiento se tiene que dar, de forma que no se pueda interpretar de distintas formas o de lugar a juicios diversos.

expreso cuando se vayan a tratar datos especialmente protegidos[261], requiriendo, además que se otorgue por escrito cuando se traten datos relativos a la ideología, creencia y religión de la persona. En el Repertorio de Recomendaciones prácticas de la OIT sobre la protección de datos de carácter personal de los trabajadores se establecen pautas acerca de la prestación del consentimiento: "*Si resultara necesario recabar datos personales facilitados por terceros, se debería informar por adelantado al trabajador, que habrá de dar su consentimiento explícito. El empleador debería indicar la finalidad del tratamiento de los datos, las fuentes y los medios que se propone utilizar, el tipo de datos que vayan a acopiarse, y las consecuencias, si las hubiere, de negar el consentimiento*[262]".

Así pues, independientemente de la fórmula prevista para la prestación del consentimiento, éste se presenta como necesario para iniciar cualquier tipo de tratamiento de datos de carácter personal. El hecho de que la LOPD sólo haya establecido la prestación de un consentimiento inequívoco o expreso para los datos especialmente protegidos ha planteado algunas dudas acerca de la admisibilidad de algunas declaraciones de voluntad para el tratamiento de datos, aceptándose por algunos autores el consentimiento presunto[263], y por otros, el tácito[264].

[261] Art. 7.3 y 7.4 de la LOPD: "*Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. Sólo con consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento automatizado los datos de carácter personal que revelen la ideología, religión y creencias".*

[262] Repertorio de Recomendaciones prácticas de la OIT sobre la protección de datos de carácter personal de los trabajadores, 1997, disponible en http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf. Reunión de la Organización Internacional del Trabajo de 7 de octubre de 1996 (OIT/96/29) [Consulta 22/04/2015].

[263] Según VELASCO GÓMEZ, "*el consentimiento presunto es aquel que se produce cuando el silencio puede considerarse como un acto de aceptación*", en "Los principios de protección de datos", Boletín del Ilustre Colegio de abogados de Madrid, núm. 35, pág. 194. APARICIO SALOM establece que la forma presunta *no es una declaración de voluntad propiamente dicha, sino más bien una manifestación que permite que se deduzca esa voluntad de su comportamiento* en *Estudio sobre la protección*…, op. cit., pág.150.

[264] Según DAVARA RODRÍGUEZ, la admisibilidad del consentimiento tácito va unido a que se cumpla con el deber de información, porque éste no puede quedar exento de la información debida al titular del dato sobre el tratamiento que se le va a dar al mismo, en *La nueva Ley de*..., op. cit., pág. 23.

En el ámbito laboral, el ejemplo más claro de que el consentimiento ha sido presunto es la cumplimentación de algún formulario para participar en un proceso de selección, por ejemplo, sin autorizar el tratamiento y cesión de datos, pero siendo informado sobre el destino y uso que se le va a dar a esa información. En estos supuestos no se puede certificar la prestación del consentimiento de forma expresa pero sí la existencia del mismo, ya que está implícito en la mera facilitación de los datos por el interesado[265]. Sobre el consentimiento tácito, admitido por la doctrina[266], se puede plantear algún problema a la hora de probar ese asentimiento, puesto que éste no se deduce de actuaciones del interesado, sino más bien de su inactividad o silencio. En lo que a la protección de datos se refiere, la normativa, recoge alguna referencia al consentimiento tácito en el art. 14 del RDLOPD[267], el cual lo autoriza para aquellos casos en los que no se exija un consentimiento expreso. Sin embargo, el Grupo de Trabajo del art. 29[268] se ha manifestado en contra de la admisibilidad de esta forma de consentir tácitamente, partiendo de que el consentimiento que contempla la Directiva 95/46/CE descansa en la palabra

[265] Sentencia de la Audiencia Nacional, de 15 de octubre de 2012 (JUR 2012\342116):*"…Y ello por considerar que sí ha existido en el presente supuesto un consentimiento tácito de la afectada, o más exactamente, un consentimiento presunto, en cuanto el mismo se deduce de un comportamiento o conducta que implica aceptación de un determinado compromiso u obligación, teniendo en cuenta que la parte actora tenía el nombre y apellidos de la denunciante, sí como el número de la cuenta bancaria, pero especialmente diversas facturas todas las cuales fueron cargadas y abonadas en la cuenta bancaria titularidad de la denunciante, a excepción de las correspondientes a julio y agosto de 2008, que fueron devueltas. En concreto, fueron abonadas desde el mes de febrero de 2007 hasta el mes de junio de 2008, ambos inclusive, por importes que varían entre 7,11 euros y 23,20 euros. Es cierto que constituye doctrina reiterada y consolidada de esta Sala que, por regla general, corresponde a quien realiza el tratamiento estar en condiciones de acreditar que ha obtenido el consentimiento del afectado pues, salvo las excepciones establecidas en la Ley, sólo el consentimiento justifica o legitima el tratamiento, y a tal fin deberá arbitrar los medios necesarios para que no quepa ninguna duda de que efectivamente tal consentimiento ha sido prestado".*

[266] Para SERRANO PÉREZ, resulta posible que el consentimiento sea tácito sin que esto pueda acarrear la generalización del mismo, es decir, *"el consentimiento se presta atendiendo a cada circunstancia para la que se solicitan los datos*", y expresa la autora la posibilidad de que el consentimiento sea también presunto teniendo en cuenta la definición del mismo como libre e informado en *El derecho fundamental*…, op. cit., pág. 201. En el mismo sentido APARICIO SALOM, expone que "*el consentimiento tácito es una forma más del consentimiento presunto o implícito, que se diferencia por el hecho de que la deducción de la voluntad no se obtiene de actos del interesado, sino de su silencio*" en *Estudio sobre la protección…,* op. cit., pág. 151.

[267] Art. 14 del RDLOPD: "*El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este art., salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos".*

[268] WP 187 del Grupo de Trabajo del art. 29, disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf. [Consulta 24/04/2015].

"*manifestación*", por lo que cualquier deducción que trate de realizarse de una falta de actuación del interesado está fuera de lo que debe entenderse por consentimiento.

En este sentido, la recogida del consentimiento a través de los buscadores de empleo ha traído algunos problemas que se analizarán en el siguiente capítulo -dedicado al análisis de la intermediación laboral y la protección de datos de carácter personal. En concreto, se puede decir que una vez que se introducen los datos en los buscadores de empleo, se otorga el consentimiento para tratarlos; pero si es necesario completar la información en cualquier otro momento, entonces el consentimiento suele ser tácito pues no es necesario prestarlo cada vez que se modifica el perfil ya creado, sino que se deduce de la falta de actuación del interesado, es decir, de su silencio ante los posibles tratamientos de la nueva información añadida. Sobre este asunto, la AEPD ha elaborado el Informe Jurídico 93/2008[269], en el que se expresa: "*En cuanto al consentimiento informado, este habrá de recabarse de tal forma que resulte imposible la introducción de dato alguno sin que previamente el afectado haya conocido la advertencia que contenga las menciones a las que nos hemos referido, pudiendo servir como prueba del consentimiento la acreditación de que el programa impide introducir los datos sin antes haber aceptado el aviso legal al que hemos hecho referencia. Todo ello tiene por objeto asegurar que el consentimiento de los afectados sea efectivamente específico e inequívoco tal y como exige la Ley[270]".*

A pesar de la interpretación que la nueva normativa sobre protección de datos ha dado al consentimiento, no se ha producido una mejora respecto a lo previsto en la anterior norma. Como es lógico, no tiene sentido establecer ninguna forma de prestación del consentimiento si ésta exigencia no está así prevista en la LOPD. Ello, sin duda, supone un problema fundamental pues se

[269] Informe Jurídico 93/2008 de la AEPD, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2008-0093,[Consulta 21/04/2015].

[270] APARICIO SALOM, J: *Estudio sobre la protección…,* op. cit., pp.118-123, pp.127-128; SÁNCHEZ BRAVO, A: "La Ley Orgánica 15/1999, de Protección de datos de carácter…, op. cit., pp. 208-210.

produce una minoración de la protección de la intimidad del titular de los datos que podría verse solventada si la norma hubiera acordado un medio de prestación del consentimiento que fuera más certero que el simple hecho de que se preste de manera inequívoca. Hoy día es cierto que, si este consentimiento no se ha recogido de forma escrita, existen otros mecanismos a través de los cuales queda grabado el asentimiento para tratar los datos; como puede ser la prestación de conformidad generada por medio de la inscripción de los datos en cualquier página web, aspecto por otra parte imprescindible para solicitar algún servicio ofertado por Internet.

No obstante, la propia LOPD prevé otras habilitaciones para el tratamiento de información sin necesidad de que medie el asentimiento, como puede ser, entre otras, el caso de los datos de carácter personal que se refieran a las partes de un contrato o precontrato de una relación laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento[271]. Esta excepción al consentimiento no significa que se puedan tratar los datos sin consentimiento, sino que se entiende que su prestación está implícita en la perfección del contrato. Ahora bien, esta excepción al consentimiento debe medirse en términos de razonabilidad, es decir, que el tratamiento de datos sin asentimiento inequívoco por parte del titular sea el único medio para el mantenimiento de una relación prelaboral o laboral.

En lo que a las relaciones de trabajo se refiere se podría justificar esa falta de consentimiento en la existencia de una declaración de voluntad del trabajador previa al momento de formalización del contrato[272]. Con esta habilitación legal el empresario podrá tratar los datos personales de los

[271] Art. 6.2 de la LOPD: "*No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del art. 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".*

[272] VIZCAÍNO CALDERÓN, V.: *Comentarios a la Ley Orgánica…,* op. cit., pp. 116-119; LESMES SERRANO, C. (coord.): *La ley de protección…,* op. cit., pp. 204-207.

trabajadores, inscritos en los ficheros de recursos humanos de la empresa, sin que necesite el consentimiento del titular del dato, siempre que su uso tenga relación con el cumplimiento de las obligaciones inherentes al contrato de trabajo; permitiendo, de esta forma, que el responsable del fichero –empresario- pueda utilizar esos datos para el desempeño de sus deberes en materia laboral.

Otra de las situaciones admitidas por la LOPD para procesar información personal sin consentimiento es la referida a la permisibilidad del tratamiento para el ejercicio de las funciones de las Administraciones públicas, así como en aquellos casos en los que la Ley disponga su tratamiento. En el entorno laboral se pueden dar alguna que otra situación en la que se exceptúe el consentimiento del trabajador para tratar sus datos argumentando el cumplimiento de obligaciones empresariales relacionadas, entre otras con la comunicación de los datos de sus trabajadores a la Administración Tributaria, amparando este tratamiento de datos en la existencia de una Ley que le impone realizar esta actividad[273].

Existe también una excepción al consentimiento para el tratamiento de aquellos datos incluidos en las denominadas fuentes accesibles al público, pudiendo justificarse esta excepción en que el consentimiento se ha otorgado previamente, precisamente para que esos datos de carácter personal se incorporen a este tipo de ficheros. Por ello se puede prescindir del consentimiento del titular del dato cuando esta información aparezca en las denominadas listas profesionales con las características citadas en la normativa sobre protección de datos señaladas en el art. 3 j) de la LOPD, teniendo en cuenta también que el trabajador ha consentido anteriormente su

[273] El trabajador está obligado a comunicar al empresario determinados datos para que estos efectúen las pertinentes retenciones en sus nóminas e ingresen estas cantidades en la Administración Tributaria, según lo establecido en el art. 88 del Real Decreto 439/2007, de 30 de marzo, por el que se aprueba el Reglamento del Impuesto sobre la Renta de las Personas Físicas y se modifica el Reglamento de Planes y Fondos de Pensiones, aprobado por Real Decreto 304/2004, de 20 de febrero (BOE núm. 78 de 31 de marzo de 2007): "*Los contribuyentes deberán comunicar al pagador la situación personal y familiar que influye en el importe excepcionado de retener, en la determinación del tipo de retención o en las regularizaciones de éste, quedando obligado asimismo el pagador a conservar la comunicación debidamente firmada".*

inclusión en esos listados. Ahora bien, habrá que matizar esta excepción, pues no se debe afirmar que esta prestación previa del consentimiento sea universal; es decir, que pueda extenderse a cualquier utilización posterior de la información pues su principal finalidad, es facilitar el conocimiento de la aptitud de ese trabajador para realizar una determinada actividad profesional, por lo que, para el tratamiento o publicación de cualquier otro dato que no sea necesario para ese objetivo, debe contarse con el consentimiento del empleado[274].

Siguiendo con las excepciones al consentimiento, se debe mencionar aquellos tratamientos de datos que se refieren a la salud de su titular. En estos casos, lo que se pretende es proteger el interés vital del afectado, por lo que no será preciso solicitar su conformidad para procesar su información[275]. Para que opere esta excepción, la utilización del dato deberá hacerse por personal sanitario sujeto al secreto profesional, o por cualquier otra persona sometida a una obligación equivalente[276].

En cuanto a revocación del consentimiento, prevista en el art.6.3 de la LOPD[277] como derecho que podrá ejercer el titular del dato siempre y cuando exista una causa justificada para ello y sin que se le atribuyan efectos retroactivos, hay que decir que se trata de un concepto bastante abstracto pues ni la propia normativa sobre protección de datos llega a aclarar que se entiende por causa justificada. Lo lógico sería pensar que la revocación puede ejercitarse cuando existan "*motivos fundados y legítimos relativos a una concreta situación personal"*, restringiéndola, simplemente, a la posibilidad de

[274] Respecto de esta excepción, APARICIO SALOM, J.: *Estudio sobre la protección*…,op. cit., pág. 184-186; SERRANO PÉREZ, M.M.: *El derecho fundamental…,* op. cit., pág. 364-373.
[275] Art. 7.6 de la LOPD; "*No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este art., cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto".*
[276] LESMES SERRANO, C(coord.): *La ley de protección…,* op. cit., pp. 207-208.
[277] Art. 6.3 de la LOPD: "*El consentimiento a que se refiere el art. podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos".*

que haya una causa que justifique esa acción[278]. En este sentido, la LOPD vuelve a ser poco clarificadora, pues no establece ninguna pauta sobre qué se entiende por justa causa y cuál es su efecto[279]. Por ello, y ante la ausencia de alguna referencia normativa ni nacional ni comunitaria que aclare este asunto, la existencia de causa justificada para la revocación se presenta como un concepto que puede conllevar, debido a su elasticidad, una cierta inseguridad jurídica. Así pues, la revocación del consentimiento podría quedar limitada a aquellas situaciones en las personas intervinientes en el tratamiento de datos tienen comportamientos contrarios a la Ley o a los derechos fundamentales del titular del dato, siendo esto causa más que suficiente y motivada para proceder a la revocación[280]. No obstante, no se entiende cual es el objetivo de la LOPD estableciendo una justa causa para revocar el consentimiento pues éste se ha prestado libremente y lo lógico sería que se pudiera revocar sin que mediara ningún motivo si, además, no le produce especiales beneficios al afectado.

La normativa sobre protección de datos tampoco dice nada sobre quién tendrá que admitir esta actuación del titular del dato, dejando entrever que lo más seguro es que la posibilidad de autorizar la revocación del consentimiento provenga de lo que establezca el encargado del fichero y del tratamiento[281]. Esta revocación del consentimiento debe ir acompañada del ejercicio del derecho de cancelación, pues no tiene sentido negarse a un tratamiento de datos si estos están aún en el fichero que se creó con ese objetivo[282].

---

[278] PALACIOS GONZÁLEZ, M.D.: *"El poder de autodeterminación de los datos personales en Internet" IDP, Revista de Derecho, Internet y Política*, núm. 14, 2012, pp. 66-67.

[279] En palabras de ÁLVAREZ-CIENFUEGOS SUAREZ, *"La causa justificada" para adoptar esta decisión ha de interpretarse en sentido favorable al afectado"* en *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Aranzadi, 1999, pág.35. A estos efectos, la regulación de la revocación como consecuencia de las carencias que tiene es duramente criticada por SÁNCHEZ BRAVO en "La Ley Orgánica 15/1999, de…" op. cit. pág. 208.

[280] FERNÁNDEZ LÓPEZ, J.M.: "Principio de consentimiento" en TRONCOSO REIGADA, A.: *Comentario a la Ley Orgánica…,* op. cit*.,* pp. 470-471; ORTÍ VALLEJO, A.: *Derecho a la intimidad e informática*, Comares, 1994, pp. 145-149.

[281] Sobre este aspecto, y reafirmando la teoría de que la revocación del consentimiento no debe ir acompañada de ninguna otra condición que la refuerce, SERRANO PÉREZ, señala que: "*parece sorprendente que alguien ajeno al interesado, como es el encargado del tratamiento, pueda valorar los motivos que llevan a la persona a la persona a definir de nuevo, aunque de modo negativo, su voluntad*" en *El derecho fundamental…,* op. cit., pág. 207.

[282] Diversas son las Sentencias de la Audiencia Nacional que confirman resoluciones de la AEPD que sancionan a los responsables del fichero por seguir utilizando los datos con posterioridad a la revocación, a modo de ejemplo vid., Sentencia de la Audiencia Nacional, de

Por ejemplo, la revocación del consentimiento trasladada al plano de las relaciones de trabajo podría no tener mucho sentido sí el titular del dato, que previamente ha facilitado esa información al empresario, pretende ejercerla, ya que esos ficheros con datos tienen como única finalidad mantener ese contrato de trabajo, por lo que no sería muy recomendable, entonces, revocar el consentimiento para el tratamiento de datos si el contrato está aún vigente. Pero, en estos casos se vuelve a manifestar la posición de inferioridad jurídica que el trabajador tiene en la relación de trabajo respecto del empresario, pues es evidente que puede tener menos facilidad, si así lo decidiera, de ejercitar ese derecho quizás por el miedo a perder su puesto de trabajo si hace peticiones de este tipo al empresario, estén fundamentadas o no.

3.4. Derechos relativos a la protección de datos de carácter personal.

Los denominados derechos ARCO[283] son el conjunto de acciones a través de las cuales una persona física puede ejercer el control sobre sus datos personales. Estos derechos se regulan en los Título III de la LOPD y del RDLOPD y se idean como garantías personalísimas, es decir, que tan sólo pueden ser ejercidos por el titular de los datos[284], por su representante legal, o por un representante acreditado; de forma que el responsable del fichero puede denegar estos derechos cuando la solicitud sea formulada por persona distinta del afectado y no se acredite que actúa en su representación[285]. Se trata también de un derecho gratuito, sobre el cual el responsable del fichero no podrá fijar ningún precio para que se haga efectivo[286]. En este sentido, lo que

25 de octubre de 2012 (JUR 2013\54501) y Sentencia de la Audiencia Nacional de 3 de diciembre de 2010 (JUR 2010\413684).

[283] Derechos de acceso, rectificación, cancelación y oposición regulados en los arts. 15 y 16 de la LOPD y 27-36 del RDLOPD.

[284] Sobre este aspecto vid., Instrucción 1/1998 de la AEPD, de 19 de enero (BOE núm. 25, de 29 de enero de 1998, pág. 3058 y ss.

[285] Art. 23 del RDLOPD: "*Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado".*

[286] Art. 17.2 de la LOPD: "*No se exigirá contra prestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación".* Art. 24.2 y 3 del RDLOPD: "*2.Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. 3. El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso*

se pretende es que el titular del dato pueda ejercer su derecho de la forma más fácil posible, incluso se ha previsto en el RDLOPD[287] que, si el responsable del fichero dispone de un servicio de atención al cliente o centro de reclamaciones, los interesados puedan a través de ellos solicitar el acceso a sus datos[288]. No obstante, puede ocurrir que al ejercitar estos derechos no se obtenga respuesta del responsable del fichero, dando lugar a la interposición por parte del interesado de la reclamación contemplada en el art. 18 de la LOPD[289].

La práctica de estos derechos se debe llevar a cabo mediante medios sencillos y gratuitos puestos a disposición por el responsable del fichero el cual está obligado a informar a los trabajadores de la existencia de estos derechos y de los procedimientos habilitados para su ejercicio. A estos efectos, si cualquier ciudadano o un trabajador no ven cumplidas sus expectativas respecto al ejercicio de estos derechos, puede acudir a la tutela de la Agencia Española de Protección de Datos (AEPD)[290].

El primero de los derechos tratado por la normativa sobre protección de datos de carácter personal es el de acceso[291], cuyo objeto es facilitar al titular

---

podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan".

[287] Art. 24.4 del RDLOPD: "*Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos".*

[288] ZABIA DE LA MATA, J.: *Protección de datos…,* op. cit., pág. 268; ALMUZARA ALMAIDA, C. (coord.) *Estudio práctico sobre la protección de datos de carácter personal*, Lex Nova, 2005, pp. 123-124.

[289] Art. 18 de la LOPD: "*Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine. 2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación. 3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses. 4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo".*

[290] FERNÁNDEZ DOMÍNGUEZ, J.J. Y RODRÍGUEZ ESCANCIANO, S.: *Utilización y control de los datos…,* op. cit*.,* pp. 224-242.

[291] Art. 15 de la LOPD: "*El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.2. La*

del dato información sobre: el origen de los datos contenido en el fichero; la finalidad del tratamiento que, en su caso, se esté realizando; así como de las cesiones o comunicaciones de datos previstas, ya sean con consentimiento del titular o aquellas para las cuales no se exige. Este derecho, a diferencia del derecho de consulta[292], permite al interesado, y no a cualquier persona, comprobar la exactitud y veracidad de los datos almacenados, entrando con más detalle en todo lo relativo al tratamiento de datos que se va a efectuar.

El RDLOPD perfecciona la definición del art. 15 de la LOPD para aproximar este concepto de acceso a lo establecido en el art. 12 a) de la Directiva 95/46/CE[293]. La norma comunitaria establece una definición más amplia y realiza una explicación detallada del contenido de este derecho, completando la información que debe dársele al interesado en lo relativo a la conservación de los datos, el derecho a solicitar la rectificación, cancelación u oposición al tratamiento y del derecho a reclamar ante la autoridad de control y los datos de contacto de ésta[294].

Cuando el titular del dato solicita información sobre el origen de los datos ante el responsable del fichero, éste tendrá que dársela, aunque estas

---

información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. 3. El derecho de acceso a que se refiere este art. sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes".

[292] Art. 14 de la LOPD: "Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita".

[293] Art. 12 a) de la Directiva 95/46/CE: "*Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos; el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del art. 15".*

[294] VIZCAÍNO CALDERÓN, M.: *Comentarios a la Ley Orgánica*…, op. cit., pp. 193-196; LESMES SERRANO, C. (coord.): *La ley de protección…,* op. cit., pp. 342-372; APARICIO SALOM, J.: *Estudio sobre la protección*…, op. cit., pp. 294-299.

informaciones se hayan conseguido por medio de fuentes accesibles al público[295]. Hay que señalar, además, que no se hace referencia al derecho del afectado a conocer quién ha tratado esos datos, para lo que la AEPD ha establecido que el derecho de acceso no abarca la facultad de conocer las personas que han tratado esos datos dentro del ámbito de organización del responsable del fichero[296].

Hay ocasiones en las que puede resultar complicado localizar los datos y es en estos casos cuando el responsable del fichero puede solicitar al titular del dato que concrete o especifique los ficheros sobre los cuales quiere ejercitar el acceso[297]. En este sentido, la jurisprudencia ha establecido que no se puede obligar al interesado a una completa identificación, pero sí a aclarar algunos datos que ayuden a la identificación del fichero[298].

Lógicamente, la LOPD y el RDLOPD[299] hacen referencia a la facultad que tiene el titular del dato de conocer las comunicaciones a terceros que se vayan a realizar de su información personal. Ahora bien, nada dice la normativa sobre la si el interesado tiene derecho a conocer qué personas van a acceder a sus datos de carácter personal. Sobre este aspecto la jurisprudencia[300] ha concluido que este derecho de acceso podría completarse con el conocimiento de las cesiones o transmisiones de datos realizadas por encargado del tratamiento, aunque lo más lógico sería pensar que el interesado no debería de

---

[295] Resolución AEPD 1547/2009, de 16 de marzo, disponible en http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2009/common/pdfs/TD-01547-2008_Resolucion-de-fecha-16-03-2009_Art-ii-culo-15-LOPD.pdf.[Consulta 13/ 02/2015].

[296] Informe AEPD 167/2005, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/nformes_juridicos/derecho_acceso_rectificacion_cancelacion_oposicion/common/pdfs/2005-0167_Naturaleza-y-alcance-del- derecho-de-acceso.pdf. [Consulta 13/02/2015].

[297] Art. 27.2 de la LOPD: "*En virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento. No obstante, cuando razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos".*

[298] Sentencia de la Audiencia Nacional de 21 de abril de 2004 (RJCA 2004\809).

[299] Art. 27.1 del RDLOPD: "*El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos".*

[300] Sentencia de la Audiencia Nacional de 9 de junio de 2004(JUR 2004\253577).

tener acceso a esos datos, si ya previamente conoce y ha consentido esas cesiones a terceros con la finalidad de contribuir a cumplir el objetivo del tratamiento[301].

El responsable del fichero tendrá que atender a la solicitud de acceso que resolverá en el plazo máximo de un mes a contar desde la recepción de la solicitud, haciéndose efectivo el acceso durante 10 días hábiles tras la comunicación de la resolución. Si se denegara el acceso, esta denegación tendrá que motivarse e indicar que cabe invocar la tutela de la AEPD. Son motivos de denegación: que el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud (salvo que se acredite un interés legítimo al efecto); que esta situación esté prevista en una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso; que la solicitud de acceso no provenga del afectado ni de su representante, actuando esta denegación como medio de control ante el posible ejercicio por persona distinta del titular del dato[302].

---

[301] Sobre el contenido del derecho de acceso, véase: PALOMAR OLMEDA, A. (coord.): *Comentario al Reglamento de desarrollo…,* op. cit*.,* pp. 306-307; SAN JOSÉ, C.: "Les garanties del ciutadan: tutela de drets ARCO i regim sancionador" en MARICARDONA, J. Y VILASAU SOLANA, M.: *El Reglamento de protección de datos de carácter personal. Aspectos claves,* Editorial UOC, 2008, pp. 172-173.

[302] Aunque el derecho de acceso está previsto en todas las leyes de protección de datos europeas, hay algunas legislaciones como la portuguesa contempla un derecho a la información distinto al de recogida de los datos y que se ejercita con carácter previo al derecho de acceso. En esta normativa lo que se pretende es relacionar la información previa con la existencia de algún dato personal de la persona que quiere acceder a ese fichero, pues si éste no contiene ningún dato de carácter personal se desvirtúa la puesta en práctica de este derecho. Por tanto, la ley lusa distingue un derecho de acceso a la información y un ejercicio del derecho de acceso, como se puede extraer de lo contenido en el art. 11 de la Lei nº 67/98, de 26 de Outubro, Lei da protecção de dados pessoais: "*1 El interesado tiene derecho a obtener del responsable del tratamiento, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: a) La confirmación de si o no datos que les conciernen, así como información sobre los fines del tratamiento, las categorías de datos en cuestión, y los destinatarios o categorías de destinatarios a quienes se comuniquen los datos; b) comunicación en forma inteligible de objeto del tratamiento de los datos y de la información disponible sobre el origen; c) conocimiento de la lógica utilizada en el tratamiento automatizado de los datos que le conciernen; d) La rectificación, supresión o bloqueo de los datos tratados, no cumple con las disposiciones de esta ley, en particular debido al carácter incompleto o inexacto de los datos; e) notificación a los terceros a quienes los datos han sido revelados de toda rectificación, supresión o bloqueo efectuado de conformidad con el inciso d), si no resulta imposible"*. También la legislación alemana ha incluido alguna matización relativa a la falta de contemplación de este derecho de forma expresa en la ley, ya que se refiere tan sólo a la rectificación, cancelación y oposición, pero se sobreentiende que se reconoce el derecho de acceso como previo a todos ellos, como establece el art.19 de la Ley federal de protección de

Los derechos de rectificación y cancelación constituyen aspectos fundamentales del derecho a la protección de datos, pues sin ellos el interesado perdería la facultad de disposición de sus datos, quedando limitado el conocimiento del tratamiento de datos tan sólo al derecho de acceso. Aun así, la norma define estos derechos de forma confusa, ya que están incluidos dentro de un mismo precepto, el art. 16 de la LOPD[303], configurándolo como un único derecho pero con dos formas distintas de manifestarse[304]. Por un lado, la LOPD precisa el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos, permaneciendo una vez que se hayan corregido en la base de datos, y, por otro, la posibilidad de cancelar o suprimir la información del fichero. Este aspecto parece estar corregido en el RDLOPD[305] pues se alude a dos derechos diferenciados, al igual que ocurre en la citada Instrucción 1/1998 de la AEPD[306] y, aunque es obvio que se trata de

---

datos de 14 de enero de 2003 reconociendo al afectado un derecho a la información: "*Si así lo pidiere, deberá darse información al afectado acerca de: 1) los datos almacenados sobre su persona, incluso en la medida en que la información hiciere referencia al origen o los cesionarios de los datos, y 2) la finalidad del almacenamiento. En la petición deberá detallarse la naturaleza de los datos personales sobre los cuales debiere darse la información. Si los datos personales estuvieren almacenados en expedientes, la información sólo se dará si el afectado diere indicaciones que hicieren posible la búsqueda de los datos, y si el coste de la dación de la información no fuere desproporcionado en relación con el interés alegado por el afectado para pedir la información. El organismo almacenante determinará, a su discreción, el procedimiento, en especial la forma de dar la información".*

[303] Art.16 de la LOPD; "*1.El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos. 3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado".*

[304] La relación de estos derechos es un aspecto que ha puesto de manifiesto LUCAS MURILLO DE LA CUEVA, P: *El derecho a la…,* op. cit., pág.187; REBOLLO DELGADO, L. Y SERRANO PÉREZ, M.: *Introducción al derecho a la protección de datos*…, op. cit., pág.191; PÉREZ DE VELASCO J.R.: "Protección de datos de carácter personal", *Revista Española de Derecho Internacional*, núm. 27, 2000, pág.5

[305] Art. 31 del RDLOPD: "*1. El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos. 2. El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento".*

[306] Norma Tercera de la Instrucción 1/1998 de la AEPD, de 19 de enero, sobre los derechos de acceso, rectificación, cancelación y oposición (BOE núm. 25 de 29 de enero de 1998): "*Si los*

dos derechos distintos, también es lógico que en algún momento su aplicación haya podido dar lugar a algún tipo de confusión, sobre todo teniendo en cuenta que si el dato se corrige o se rectifica evidentemente se está cancelando, ya que da lugar al almacenamiento de un nuevo dato en el fichero como consecuencia de esa modificación[307].

No obstante, existen referencias en la normativa sobre protección de datos relativas al bloqueo de los datos para aquellos supuestos en los que deban de conservarse para atender alguna reclamación judicial o administrativa[308]. Por tanto, en estos supuestos la cancelación no significaría la supresión total de la información del fichero pero, sí la prohibición de usarla o tratarla, ya que transcurrido el plazo fijado para atender los requerimientos administrativos y judiciales, estos datos bloqueados serán eliminados definitivamente del fichero. Además, la AEPD[309] contempla también algún supuesto en el que la cancelación no puede ser operativa por razones físicas, o como consecuencia del tipo de soporte en donde estén ubicados los datos, para los que recomienda la destrucción de ese soporte con el fin de eliminar la información personal allí contenida, siempre que este sea el único medio

---

datos de carácter personal del afectado son inexactos o incompletos, inadecuados o excesivos, podrá éste solicitar del responsable del fichero la rectificación o, en su caso, la cancelación de los mismos".

[307] En este sentido: HERRÁN ORTIZ, A.I.: *La violación de la…*, op. cit., pág. 288; FREIXAS GUTIÉRREZ, G.: *La protección de los datos de carácter personal en el derecho español*, Bosch, 2000, pág. 197; VIZCAÍNO CALDERÓN, M.: *Comentarios a la Ley Orgánica…,* op.cit., pp. 199-201; SANTOS GARCÍA, D.: *Nociones generales dela…*, op.cit., pp. 108-114.

[308] Art.16.3 de la LOPD: "La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposició*n de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión".* Art. 5.1.b) del RDLOPD: "*Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos".*

[309] Norma Tercera de la Instrucción 1/1998 de 19 de enero sobre los derechos de acceso, rectificación, cancelación y oposición: "*En los casos en que, siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el responsable del fichero procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización. Se exceptúa, no obstante, el supuesto en el que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren".*

posible para poder suprimir los datos del fichero y que no exista otro modo menos invasivo.

Para poder ejercer los derechos de rectificación y cancelación se tiene que dirigir una solicitud al responsable del fichero con el contenido citado en el art. 25.1 del RDLOPD[310], siendo el plazo en el que se debe realizar la rectificación o cancelación de datos de 10 días hábiles[311], tiempo máximo para resolver la solicitud de rectificación o cancelación[312].

Cabe hacer un inciso para tratar el derecho de conservación de los datos de carácter personal como garantía para que no opere su cancelación, algo sobre lo que ha intervenido el TJCE[313] en una resolución acerca del derecho de conservación de los datos, que anula la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE[314]. El TJCE considera que, al imponer la conservación de estos datos y al permitir el acceso a las autoridades nacionales competentes, la Directiva se inmiscuye de manera especialmente grave en los derechos fundamentales de respeto de la vida privada y a la protección de datos de

[310] Art. 25.1 del RDLOPD: "*Salvo en el supuesto referido en el párrafo 4 del art. anterior, el ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá: a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente. El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos. b) Petición en que se concreta la solicitud. c) Dirección a efectos de notificaciones, fecha y firma del solicitante. d) Documentos acreditativos de la petición que formula, en su caso".*

[311] Art. 16.1 de la LOPD: "*El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días".*

[312] Art. 32.2 del RDLOPD: "*El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el art. 18 de la Ley Orgánica 15/1999, de 13 de diciembre. En el caso de que no disponga de datos de carácter personal del afectado deberá igualmente comunicárselo en el mismo plazo".*

[313] Sentencia del TJCE de 8 de abril de 2014 (Asunto C-293/12 y C-594/12).

[314] DOUE núm.105 de 13 de abril de 2006.

carácter personal. Además, el hecho de que la conservación y la utilización posterior de los datos se hagan sin que el abonado o el usuario registrado sea informado de ello, puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante. Considera asimismo que la Directiva no contiene garantías suficientes que permitan asegurar una protección eficaz de los datos contra los riesgos de abuso y contra cualquier acceso y utilización ilícitos de los datos.

Y por último, el derecho de oposición aparece en la LOPD de forma innovadora –aunque tan sólo hace referencia a el procedimiento para ejercitarlo- pues no estaba contemplado en la LORTAD y tan sólo se trataba de forma específica en el RDLOPD como una acción que puede ejercer el interesado cuando pretenda que no se lleve a cabo el tratamiento de sus datos de carácter personal. De lo contenido en el RDLOPD parece deducirse que es un derecho que puede ejercer el interesado: cuando se niegue a que sus datos sean objeto de tratamiento invocando algún motivo legítimo; cuando se trate de ficheros de prospección comercial; o cuando el tratamiento estos tenga la finalidad de adoptar decisiones referidas al interesado que únicamente puedan llevarse a cabo con el procesamiento automatizado de sus datos[315].

La Directiva 95/46/CE establece un concepto de oposición[316] un poco más preciso que el establecido en el RDLOPD pues habilita al titular del dato a oponerse al tratamiento legítimo de sus datos. Es decir, a diferencia de lo establecido en la RDLOPD, la Directiva 95/46/CE expone que el derecho de

[315] Art. 34 del RDLOPD: "*El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos: a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario. b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el art. 51 de este reglamento, cualquiera que sea la empresa responsable de su creación. c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el art. 36 de este reglamento".*

[316] Considerando 45: *"…cuando se pudiera efectuar lícitamente un tratamiento de datos por razones de interés público o del ejercicio de la autoridad pública, o en interés legítimo de una persona física, cualquier persona deberá, sin embargo, tener derecho a oponerse a que los datos que le conciernan sean objeto de un tratamiento, en virtud de motivos fundados y legítimos relativos a su situación concreta; que los Estados miembros tienen, no obstante, la posibilidad de establecer disposiciones nacionales contrarias".*

oposición sólo procede en tratamientos de datos legítimos pudiéndolo ejercer el interesado, siempre que este derecho esté fundado en alguna causa o motivo fundado y legítimo[317].

Ante la falta de regulación de este derecho de oposición en la LOPD tan sólo reglamenta el procedimiento, como se ha visto, y alguna referencia hace en su art. 6.4[318]- es el RDLOPD[319]el que lo regula, debiendo iniciarse de la misma forma que los anteriores derechos aludidos, es decir, con una solicitud que deberá dirigir el titular del dato al responsable del tratamiento. El plazo para resolver la solicitud de oposición será también de diez días desde su recepción, obligando la norma al responsable a motivar su denegación debidamente, pudiendo el interesado, si lo estima oportuno, interponer la reclamación contemplada en el art. 18 de la LOPD[320].

4. OBLIGACIONES IMPUESTAS A LOS SUJETOS ENCARGADOS DE LOS FICHEROS DE DATOS.

La LOPD establece una serie de limitaciones al tratamiento de los datos, fijadas para garantizar un uso adecuado, lícito y no excesivo para impedir su alteración, pérdida o tratamiento no autorizado. Como se conoce, el tratamiento de datos no es un acto que tenga eficacia universal, ya que tiene sus

[317] APARICIO SALOM, J.: *Estudio sobre la protección*…, op. cit., pp.303-305.
[318] Art. 6.4 de la LOPD: "*En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable de fichero excluirá del tratamiento los datos relativos al afectado".*
[319] Art. 35 del RDLOPD: "*1. El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento. Cuando la oposición se realice con base en la letra a) del art. anterior, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho. 2. El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el art. 18 de la Ley Orgánica 15/1999, de 13 de diciembre. En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo. 3. El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo previsto en el apartado 2 de este art.*".
[320] CARDONA RUBERT, M.B.:" Derechos de acceso, rectificación, cancelación y oposición" en VV.AA*.: Protección de datos: comentarios a la LOPD y su reglamento de desarrollo*, Tirant lo Blanch, 2009, pp. 201-217; GONZÁLEZ TAPIA, M.L.: "El derecho de oposición" *Datos personales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, núm. 25, 2007; SERRANO PÉREZ, M.M.: *El derecho fundamental…,* op. cit., pp. 369-373.

limitaciones, basadas principalmente en el uso del tratamiento de datos como único medio para poder desarrollar una determinada actividad o prestar un servicio al titular del dato.

Desde la implantación de las TICS las entidades que tramitan datos personales manejan y procesan una gran cantidad de información personal de forma más rápida y eficaz, por lo que deben cumplir una serie de obligaciones para restringir así un tratamiento de datos que no sea acorde con lo establecido en la normativa sobre protección de datos de carácter personal. En primer lugar, esta entidad, como responsable del fichero, tendrá que legalizar el fichero de datos de carácter personal inscribiéndolo en el Registro General sito en la AEPD[321], el cual establece una serie de ficheros distintos dependiendo del tipo de datos que se quiera registrar[322], catalogando los tipos de ficheros existentes y analizando no sólo la finalidad para la que son tratados los datos, sino también el origen de la información y el sistema de almacenamiento que se usa en la entidad. En segundo lugar, tendrán que atender a los citados principios de la protección de datos cuyo cumplimiento es esencial para una correcta gestión de datos de carácter personal y por último, se deberán establecer unas correctas medidas de seguridad atendiendo a la importancia de los datos contenidos en el fichero para proteger la información personal de posibles incidencias que puedan provocar su pérdida, alteración o acceso no consentido.

4.1. Breve referencia a los sujetos encargados de la protección de datos.

Al margen de lo dicho sobre el tratamiento de datos, lo primero que hay que especificar es que las obligaciones, concretadas en la LOPD, las tendrán que cumplir los entes que traten datos de carácter personal. Es obvio que en la

[321] Esta inscripción tendrá que hacerse conforme a lo establecido en los arts. 25 y 26 de la LOPD.

[322] Así mismo, permite notificar de forma simplificada una serie de ficheros de titularidad privada relacionados con la gestión de comunidades de propietarios, clientes, libro recetario de las oficinas de farmacia, pacientes, gestión escolar, video vigilancia, nóminas y recursos humanos y por otra parte, los de titularidad pública relativos a la gestión del padrón, gestión económica o control de acceso. En el caso de que ninguna de las notificaciones tipo previstas por la AEPD se adapte al fichero que se pretende notificar, el responsable del fichero podrá seleccionar la opción de notificación normal. Fuente: *www.aepd.es.*

mayoría de empresas, incluyendo las de intermediación, el uso de la información personal forma parte de su funcionamiento diario, siendo indispensable para el desarrollo y ejecución de la actividad negocial, administrativa, fiscal, contable y/o laboral de la empresa.

Antes del inicio de su actividad, la entidad que procesa datos de carácter personal tendrá que analizar si le resulta de aplicación la LOPD, atendiendo a su ámbito objetivo definido en el citado art. 2.1 y al concepto de dato de carácter personal establecido en el art. 3 a) de la misma norma. Lógicamente, la gestión de datos realizada por las entidades a las que se va a hacer referencia a lo largo de este trabajo está dentro del ámbito de aplicación de la LOPD. Asimismo, siguiendo la definición de dato de carácter personal, la información de los trabajadores, necesaria para las actividades relacionadas con los recursos humanos de la empresa, también está dentro del entorno protegido por la LOPD. Ahora bien, si para la gestión de personal se tienen que tratar, por ejemplo, datos de proveedores, se plantea un problema debido a que muchos de ellos son personas jurídicas, las cuales no se encuentran dentro de ámbito de protección de la LOPD[323], por lo que esas informaciones no quedarían protegidas por la normativa sobre protección de datos.

En cuanto al ámbito subjetivo, definido en el art. 2.1 de la LOPD, la norma establece que el responsable del fichero encargado de la custodia de los datos y de someterlos a tratamiento es aquella "*persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*[324]*,* quien tendrá que respetar lo contenido en la normativa sobre protección de datos. En este sentido, la actividad que desarrolla el responsable del fichero será clave para concretar la finalidad del tratamiento, estando obligado por la LOPD desde el mismo momento en el que recoge los datos de carácter personal, siendo, por tanto, el

[323] Art. 2.2 del RDLOPD: "*2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales".*
[324] Art. 3. d) de la LOPD.

que debe garantizar el derecho a la protección de datos de todas las personas cuya información almacena[325].

En este sentido, y en lo que a los trabajadores se refiere, las bases de datos que los responsables del fichero tendrán que crear serán; a) en cuanto a la selección de personal: ficheros con información sobre aptitud profesional para desempeñar un concreto puesto de trabajo, sobre formación y experiencia profesional previa, disponibilidad horaria y territorial, superación de las pruebas realizadas para la selección, etc.; b) en cuanto a la gestión de personal ya contratado: datos personales para gestionar el pago de la nómina y las gestiones ante la Seguridad Social y la Administración Tributaria, información necesaria para llevar a cabo una correcta política de prevención de riesgos laborales, datos para iniciar acciones de formación en la empresa que se adapten a las necesidades formativas de cada trabajador.; y, c) en lo relativo a la extinción del contrato de trabajo, será necesario establecer ficheros con datos sobre cotización a la Seguridad Social, período de tiempo trabajado en la empresa, datos familiares, datos bancarios, etc.

Para poder controlar esa información del trabajador, independientemente de si es tratada por entes públicos o privados, el responsable del tratamiento la almacena en ficheros definidos por la LOPD como : "*el conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso por tanto, el soporte físico, sea automatizado o no, en el que se recoge y almacena, de manera organizada, el conjunto de datos que integra la información*[326]*"*. Para atender a este compromiso, ni el centro de trabajo, ni la entidad pública que trate la señalada información personal de los trabajadores, podrán ignorar lo previsto en la normativa sobre protección de datos y para ello, deben hacer constar las pautas o instrucciones para proceder a su utilización, independientemente del soporte, físico o automatizado, en que el que esté configurado el fichero.

[325] DEL PESO NAVARRO, E.: "La figura del responsable del fichero de datos de carácter personal en la L.O.R.T.A.D", *Informática y derecho: Revista iberoamericana de derecho informático*, núm. 6-7, 1994, pp. 249-270; ARIAS POU, M.: "El encargado del tratamiento y el documento de seguridad" en VV.AA.: *Derecho y Nuevas Tecnologías*, Univ. Deusto, 2011, pp.143-152.
[326] Art.3.1.b) de la LOPD.

Además, el responsable del fichero tiene que tener en cuenta otros aspectos como son: las exigencias referida al cumplimiento de los principios de protección de datos; facultar a los interesados el ejercicio de los derechos ARCO; guardar secreto sobre la información personal almacenada; inscribir el fichero ante la AEPD; e implantar en el fichero las medidas de seguridad que correspondan[327].

4.2. Significado y alcance de los ficheros de datos de carácter personal.

Como consecuencia del establecimiento de medios informáticos para la mejora de las actividades relacionadas con la gestión de datos personales, es generalizado que el tratamiento de datos se haga, normalmente almacenándolos en ficheros que tienen que respetar unas determinadas reglas de protección para salvaguardar la información personal. Por este motivo, para que el responsable del tratamiento pueda utilizar estos datos de carácter personal, tendrá que crear un fichero en el que establezca la finalidad que se le va a dar a esos datos y, dependiendo de ésta, se dividirá en distintas bases de datos. Además, se tendrá que hacer una identificación de la persona que ostenta el cargo de responsable del fichero para que el trabajador pueda ejercer ante él los derechos reconocidos por la LOPD.

Una de las obligaciones básicas, establecidas por la LOPD, es la legalización o inscripción de los ficheros de datos de carácter personal ante la AEPD[328]. Para realizar correctamente esta inscripción es necesario cotejar, previamente, la localización y determinación de los ficheros preexistentes, así como la de los nuevos ficheros a inscribir. Por tanto, se tendrá que considerar qué fichero se quiere crear y cuál va a ser su finalidad, comprobando que no está ya inscrito en el Registro General de la AEPD.

[327] SANTOS GARCÍA, D.: *Nociones generales de la…,* op. cit., pág.182.
[328] El RGPD ha eliminado la obligación de inscribir los ficheros ante la AEPD, para sustituirla por la función documental que obliga a los responsables de los ficheros a llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad con una exhaustiva información.

En el terreno empresarial se pueden producir intromisiones ilegítimas en las libertades y derechos de los trabajadores, pues los empresarios manipulan ficheros con gran cantidad de información personal, utilizándolos, en ocasiones, para fines distintos de los preestablecidos. Por este motivo, es importante tener bien delimitados los objetivos del tratamiento y el destino que se le va a dar a la información contenida en los ficheros. Por ejemplo, en las empresas de intermediación se debe acotar la finalidad de los ficheros debido a los distintos servicios[329] que se ofrecen a los demandantes de empleo y para los que, como es obvio, utilizan sus datos de carácter personal.

En lo concerniente a los ficheros y su catalogación como públicos o privados se puede interpretar, de lo establecido en la LOPD, que la determinación de su naturaleza no se fija teniendo en cuenta los datos personales que se incluyen en ellos, sino más bien el criterio que se sigue está relacionada con la institución que tiene la responsabilidad del citado fichero[330]. Así pues serán ficheros de titularidad privada, según el art. 25 de la LOPD aquellos que: "… *que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas",* siendo el único requisito que se exige para la creación del mismo su comunicación a la AEPD.

Por el contrario, serán ficheros de titularidad pública, también necesarios para llevar a cabo una correcta gestión de personal, los creados para su uso en la Administración Pública, regulados por los arts. 20 a 24 de la LOPD, los cuales sólo podrán crearse cuando lo establezca una disposición general publicada en el BOE o en el Diario oficial correspondiente. No obstante, no

[329] Entre estos servicios, además de los relacionados con la búsqueda efectiva de empleo, destacan: la gestión de bajas por incapacidad, la realización de contratos a trabajadores, comunicación de datos a empresarios y entidades públicas, etc.

[330] Sobre este aspecto la AEPD: "*Por tanto, considera esta Agencia Española de Protección de Datos que la delimitación del régimen aplicable a los ficheros de titularidad pública y privada deberá fundarse en la naturaleza de Administración Pública territorial de la responsable del tratamiento y, en los restantes supuestos, en el hecho de que el fichero haya sido creado con la finalidad de garantizar el ejercicio de potestades de derecho público."* Vid., Informe 191/2005 disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos [Consulta 08/02/2015].

podrá producirse comunicación de datos personales entre Administraciones Públicas si la cesión de datos es para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, "*salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos"* (art. 21 LOPD).

En lo que al ámbito laboral se refiere, las bases de datos que se manejan, entre otros, en los Servicios Públicos de Empleo tienen esta naturaleza pública y como tales, deben cumplir con lo establecido en la LOPD y en el RDLOPD. Si bien el significado que cabe atribuir a la expresión "*titularidad pública"* se desprende de dos posibles interpretaciones; la primera, atendiendo a un criterio subjetivo, establece que su significado dependerá de la naturaleza pública o privada del titular del fichero; y la segunda se basa en un criterio material a través del cual se atiende a la función desempeñada por el citado responsable. A estos efectos, desde la óptica de la LOPD, parece que es más acertado el criterio relativo a la naturaleza pública o privada del responsable del fichero, puesto que, como se ha visto, es lo que de la normativa sobre protección de datos puede interpretarse.

El hecho de que la LOPD contemple estos dos tipos de ficheros –públicos y privados- hace pensar que, en el caso de los trabajadores y en lo que a la gestión de recursos humanos se refiere, la creación de estas bases de datos en el seno de la empresa consiste en la creación de un fichero privado cuyo responsable y titular es el empresario; pero que, por otra parte, al ser transmitidos a órganos de la Administración Pública (Hacienda, TGSS etc.) para llevar a cabo los trámites de alta en el régimen general de la Seguridad Social o para ingresar la parte proporcional de IRPF de sus nóminas pasan a ser de naturaleza pública, ya que las entidades que los gestionan tienen esta categoría. Estos organismos, que reciben los datos de los trabajadores, mantienen bases de datos con información de los empleados de las empresas mientras dure su relación laboral, así como cuando ésta finalice y se conviertan

en sujetos con derecho a solicitar alguna prestación ante las Administraciones Públicas[331], siendo por tanto, de obligado cumplimiento los preceptos de la normativa sobre protección de datos.

Por lo expuesto, se puede afirmar que tanto los ficheros utilizados en aquellas actividades relacionadas con la intermediación laboral, siempre que se gestionen por entes privados, como los creados por las empresa con datos de trabajadores, son ficheros de titularidad privada pues se tiene en cuenta la naturaleza privada del responsable del fichero. En cambio, aquellas bases de datos que tienen como objetivo gestionar las pertinentes prestaciones de desempleados o de personas que ya han terminado su relación laboral de forma definitiva (jubilados), tienen la categoría de fichero de titularidad pública, pues el responsable del mismo será una entidad de carácter público.

4.3. Establecimiento de medidas de seguridad en los ficheros de datos de carácter personal.

Como consecuencia del almacenamiento de datos en ficheros, lo habitual es que se implanten determinadas medidas de seguridad para, de esta forma, cumplir con lo establecido en el art. 9 de la LOPD[332]. Sin duda, en este punto la entidad encargada del tratamiento de datos es la que tiene que garantizar la seguridad de los datos para evitar su alteración, pérdida o tratamiento no autorizado[333]. Las medidas de seguridad descritas en la LOPD son las denominadas de carácter técnico pero, además de éstas, existen otras

[331] VV.AA *La protección de datos en la Gestión de Empresas*, Revista Aranzadi de Derecho y Nuevas Tecnologías. Aranzadi, Pamplona, 2004. pp. 78-80; SANTOS GARCÍA, D; *Nociones generales de la…,* op. cit., pp. 127-132, 177-180.

[332] Art. 9 de la LOPD: "*El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del Estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural".*

[333] Sobre el establecimiento de medidas de seguridad en Francia la Loi nº 78-17, du 6 janvier de 1978 relative a l'informatique, aux fichiers et aux libertés (Journal officiel du 7 janvier de 1978), establece que los responsables del tratamiento informático de los datos personales están obligados a adoptar medidas de seguridad físicas, lógicas y adaptadas a la naturaleza de los datos y a los posibles riesgos que plantee el procesamiento de los mismos. Sin embargo, en la legislación española sobre protección de datos, no se distingue entre fichero automatizado o no a la hora de establecer las medidas de seguridad, exigiendo éstas para cualquier fichero, independientemente de su naturaleza.

no catalogadas que pueden llegar a realizar funciones similares se trata de las por un lado, de las medidas organizativas encaminadas a instaurar reglas para el correcto tratamiento de datos[334], como, por ejemplo, que el personal de la empresa sepa cómo debe actuar para respetar el derecho a la protección de datos, o las jurídicas, es decir, las que surgen como resultado de la aplicación de la LOPD con efectos entre los interesados o titulares de los datos, por ejemplo, la firma de contratos necesarios para el cumplimiento de la LOPD[335].

Ahora bien, para implantar las medidas de seguridad de carácter técnico contempladas en la LOPD, es necesario, en primer lugar, la elaboración del documento de seguridad en el que se recogen las pautas de seguridad dadas por el responsable del fichero que se van a implantar en todos los mecanismos que traten datos de carácter personal y que deberán cumplir todas las personas que usen esa información. En dicho documento se deberá incluir un listado en el que aparezcan todas las personas que van a tratar los datos para los cuales será de obligado cumplimiento lo contenido en el documento de seguridad.

En segundo lugar, una vez elaborado el documento de seguridad, el responsable del fichero tendrá que implantar los medios adecuados al tipo de tratamiento que se va a efectuar estableciendo las medidas de seguridad pertinentes dependiendo del tipo de datos almacenados. Es evidente que en todos los ficheros que contengan información personal se aplica alguno de los tres niveles de seguridad[336] y, en muchos de ellos, debido a la especial trascendencia de los datos que se almacenan, todos. Por este motivo, en la realización de gestiones relacionadas con los recursos humanos se tendrá que

[334] Sobre este asunto el RGPD establece en su art. 25.1 que : "*Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados".*
[335] SANTOS GARCÍA, D.: Nociones generales de la…, op. cit.,pp.187-188.
[336] Art. 80 del RDLOPD: *"Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto*".

respetar, en la preparación de los ficheros de datos personales de trabajadores, las medidas de seguridad de nivel básico, pero, si se tratan o se necesitan más datos de los catalogados como especialmente sensibles, se tendrán que complementar las medidas de nivel básico con las de nivel medio y alto[337]. El mantenimiento de datos sin las pertinentes medidas de seguridad, puede conllevar sanciones administrativas[338], tal y como se ha reconocido en sede jurisprudencial[339].

No obstante, si en los ficheros están incluidos datos relacionados con la comisión de infracciones administrativas o penales establecidas en el art. 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito); de Administraciones tributarias y que se relacionen con el ejercicio de sus potestades tributarias; de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros; de Entidades Gestoras y Servicios Comunes de Seguridad Social se adoptarán medidas de nivel medio; y las de nivel alto las utilizarán cuando los ficheros versen sobre la

[337] Según la AEPD; "*Si los ficheros de gestión de personal contienen datos de carácter personal y estos no son datos de salud, ni de ideología, afiliación sindical, religión, creencias, origen racial, no se deberá de adoptar medidas de seguridad de nivel alto. Por lo que la regla general es establecer medidas de nivel básico, teniendo en cuenta lo que señala el art. 81 del RDLOPD".* Vid., Informe jurídico 82/2008 sobre los niveles de seguridad disponible en http://www.policiacanaria.com/sites/default/files/medidas-de-seguridad-en-los-ficheros-de-n-oo-minas.pdf. [Consulta 20/01/2015].

[338] Art. 45 de la LOPD: "*1. Las infracciones leves serán sancionadas con multa de 900 a 40. 000 euros. 2. Las infracciones graves serán sancionadas con multa de 40. 001 a 300. 000 euros. 3. Las infracciones muy graves serán sancionadas con multa de 300. 001 a 600. 000 euros".*

[339] Sentencia de la Audiencia Nacional de 9 de octubre de 2006 (RJCA 2006\758): "*La Agencia de Protección de Datos considera en su resolución que el art. 9 de la LOPD (RCL 1999, 3058) establece el principio de «seguridad de los datos» imponiendo la obligación de adoptar las medidas de índole técnica u organizativa que garanticen aquella, teniendo tales medidas, entre otras finalidades, la de evitar los accesos no autorizados. En el presente caso, el empleado de Caja España accedió a ficheros cuya responsabilidad corresponde a dicha entidad crediticia, ficheros que contienen datos personales de clientes, sin disponer de la preceptiva autorización para ello. Por tanto, el objeto del procedimiento sancionador incide en las medidas de seguridad relativas a la generación de la copia no autorizada del disquete con los datos de los compromisarios de Caja España, realizada mediante el acceso indebido al fichero original cuyo responsable es Caja España. Según afirma la Administración, Caja España no prestó la diligencia debida en orden a la efectiva observancia de las medidas de seguridad implantadas pues de otro modo no se explica que un empleado de la entidad haya accedido indebidamente al fichero de compromisarios y pueda generar una copia del mismo sin que el responsable del fichero se percatara de tal conducta".*

ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual[340].

Si bien, para implantar medidas de seguridad de nivel básico habrá, además de elaborar el citado documento de seguridad, llevar un registro de incidencias; constituir una relación del personal usuario autorizado para acceder a los datos; inventariar los soportes informáticos con datos de carácter personal; almacenarlos con acceso restringido a las personas autorizadas; y determinar la forma y momento en que se realizarán las copias de los datos con un mínimo de una vez por semana salvo que no se hubieran producido cambios.

Sin embargo, si el encargado de tratar la información personal procesa datos personales clasificados de nivel medio y/o nivel alto deberá adicionalmente a las obligaciones anteriores, adoptar las medidas oportunas en atención a la naturaleza de los datos tratados. En el caso que sea necesario, deberá cumplir las siguientes obligaciones: respetar las condiciones de comunicación de datos personales; regular mediante un contrato el acceso a los datos personales por parte de un tercero para prestar un servicio al responsable del tratamiento; las transferencias internacionales de datos para las que se exige autorización previa del Director de la AEPD, salvo que concurra alguna de las excepciones[341] tasadas en la normativa sobre protección de datos de carácter personal[342].

Como consecuencia de la gran cantidad de comunicaciones electrónicas que se realizan entre empresas, la AEPD, además del mecanismo de inscripción de ficheros en su registro, ha puesto en marcha un sistema para

[340] Art. 81 del RDLOPD: Aplicación de los niveles de seguridad.
[341] Sobre este aspecto se va a incidir en el segundo capítulo, a la hora de tratar la transferencia internacional de datos como instrumento de intermediación laboral.
[342] RUBÍ NAVARRETE, J.: "Los principios de protección de datos y el reglamento de medidas de seguridad" en VV.AA.*: XIV Encuentros sobre Informática y Derecho: 2000-2001,* Aranzadi, 2001, pp. 79-86; DAVARA RODRÍGUEZ, M.: "Las medidas de seguridad de los datos" *Revista técnica especializada en administración local y justicia municipal,* núm.15-16. 2010, pp. 2420-2428; Guía de Seguridad de Datos 2010. AEPD; APARICIO SALOM, J.: *Estudio sobre la protección*…, op. cit., pp. 244-258; SANTOS GARCÍA, D.: *Nociones generales de la…,* op. cit., pp. 191-192.

que los proveedores de servicios de comunicaciones electrónicas puedan notificar a las empresas las posibles quiebras de seguridad[343] que se produzcan. Esta decisión de la AEPD tiene su fundamento en el Reglamento 611/2013, de la Comisión Europea, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas[344], y concretamente en el art. 2[345], dónde se establece cómo proceder ante las posibles violaciones relativas a la protección de datos de carácter personal, implantándose la obligación para los proveedores de notificar estas infracciones a la autoridad nacional competente (en España a la AEPD).

[343] Las quiebras de seguridad están definidas en la AEPD, como: "*toda violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizado de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público*".

[344] DOUE núm.173, de 26 de junio de 2013.

[345] Art. 2 del Reglamento 611/2013: "*1. Los proveedores notificarán todos los casos de violación de datos personales a la autoridad nacional competente. 2. En la medida de lo posible, los proveedores notificarán los casos de violación de datos personales a la autoridad nacional competente dentro de las 24 horas siguientes a la detección del caso. Los proveedores consignarán en su notificación a la autoridad nacional competente la información recogida en el anexo I. Se considerará que se ha detectado un caso de violación de datos personales cuando el proveedor tenga conocimiento suficiente de que se ha producido un incidente de seguridad que compromete datos personales para efectuar una notificación válida conforme a lo establecido en el presente Reglamento. 3. Cuando no se disponga de toda la información indicada en el anexo I y sea preciso investigar más exhaustivamente el caso de violación de datos personales, se autorizará al proveedor a enviar una notificación inicial a la autoridad nacional competente dentro de las 24 horas siguientes a la detección del caso. Esta notificación inicial incluirá la información contemplada en el anexo I, sección 1. El proveedor remitirá una segunda notificación a la autoridad nacional competente lo antes posible y, a más tardar, dentro de los tres días siguientes a la notificación inicial. En esta segunda notificación se incluirá la información indicada en el anexo I, sección 2, y, cuando proceda, se actualizará la información ya proporcionada. Cuando, a pesar de las pesquisas realizadas, el proveedor no pueda proporcionar toda la información en el plazo de los tres días siguientes a la notificación inicial, deberá notificar toda la información de que disponga dentro de ese plazo y presentar a la autoridad nacional competente una justificación motivada de la tardía notificación de la información restante. El proveedor notificará esa información restante a la autoridad nacional competente y, cuando proceda, actualizará la información ya proporcionada, en el plazo más breve posible.4. La autoridad nacional competente pondrá a disposición de todos los proveedores establecidos en el Estado miembro de que se trate un soporte electrónico seguro para notificar los casos de violación de datos personales, así como información sobre los procedimientos para acceder a dicho soporte y utilizarlo. Cuando sea necesario, la Comisión convocará reuniones con las autoridades nacionales competentes a fin de facilitar la aplicación de esta disposición. 5. Cuando una violación de datos personales afecte a abonados o particulares de Estados miembros distintos de aquel de la autoridad nacional competente a la que se haya notificado el caso de violación de datos personales, la autoridad nacional competente informará a las demás autoridades nacionales afectadas. A fin de facilitar la aplicación de esta disposición, la Comisión elaborará y mantendrá al día una lista de las autoridades nacionales competentes y los puntos de contacto correspondientes."*

El procedimiento con el que se facilita el cumplimiento de esta obligación está disponible en la sede electrónica de la AEPD a través del apartado "*notificación preceptiva de quiebras de seguridad*[346]". Los proveedores, los cuáles utilizan este mecanismo de forma exclusiva, tendrán que comunicar estas quiebras de seguridad en un plazo de 24 horas desde que tienen conocimiento del incidente. Con este medio se establece un canal rápido y seguro para reforzar las garantías de los abonados o particulares que hayan podido verse afectados por alguna quiebra de seguridad[347].

En el ámbito laboral, como se verá en el desarrollo de los distintos supuestos de protección de datos, se pueden producir también estas quiebras de seguridad, sobre todo cuando se realizan comunicaciones electrónicas a los distintos organismos de la Administración Estatal para notificar datos de los trabajadores relativos al inicio de su relación laboral, a las vicisitudes que pueden producirse en el transcurso de la misma, o aquellas que se refieran a la finalización de su contrato de trabajo. Si se producen estas quiebras, el proveedor de los servicios de comunicaciones electrónicas tendrá igualmente que notificarlo a la AEPD, siguiendo el procedimiento establecido[348].

5. INSTITUCIONES DE CONTROL DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

Las instituciones de control creadas para dar protección frente a las posibles vulneraciones que se puedan dar en el tratamiento de la información personal de los ciudadanos, son necesarias para que se haga un correcto uso de los datos de carácter personal. Las entidades encargadas de la garantía del derecho a la protección de datos de carácter personal se pueden configurar de distintas formas: en primer lugar, se pueden establecer órganos unipersonales

[346] Disponible en https://sedeagpd.gob.es/sede-electronica-web/vistas/formQuiebraSeguridad.
[347] Nota de prensa AEPD, de 23 de marzo de 2014, disponible en http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/abr_14/140423_NP_Notificacion_quiebras.pdf.
[348] NAVALPOTRO NAVALPOTRO, Y.: "Inscripción de ficheros", en ALMUZARA ALMAIDA, C. (coord.): *Estudio práctico sobre la protección de datos de carácter personal*, Lex Nova, 2005, pp. 333-358; MARTÍNEZ SÁNCHEZ, M.: "Creación, notificación e inscripción registral de ficheros de titularidad privada: Título IV. Disposiciones Sectoriales. Cap. II. Ficheros de Titularidad Privada. art.s 25 y 26" en TRONCOSO REIGADA, A. (coord).: *Comentario a la Ley Orgánica…,* op.cit*.,* pp.1457-1485.

con plena independencia en su actuación y sometidos únicamente a la ley, como puede ser el caso del Comisario Federal de Protección de Datos en Alemania[349]; en segundo lugar, se puede atribuir funciones de defensa del derecho a los tribunales ordinarios como ocurre en Estados Unidos, siendo el Tribunal Supremo Estadounidense el único que dictamina la posible vulneración del derecho; y, en último lugar, se pueden crear órganos colegiados de protección, como es, en el caso español, la Agencia Española de Protección de Datos[350].

Además de la protección prevista en la AEPD los datos de los trabajadores, tratados en el marco de la gestión de los recursos humanos, pueden encontrar también protección en los Tribunales. Así lo ha previsto la Ley 36/2011, de 10 de octubre, reguladora de la Jurisdicción Social[351] que, en su Capítulo XI regula la tutela jurisdiccional de los derechos fundamentales de los trabajadores[352], entre los que se encuentra obviamente y por lo dicho repetidamente el derecho a la protección de datos[353].

Ahora bien, en España existen distintas agencias dedicadas a controlar el buen uso de los datos de carácter personal como muestra de la descentralización territorial de la Administración, reflejada también en el campo de la protección de datos de carácter personal. En este sentido, Cataluña y el

[349] Este Comisario está integrado dentro del Ministerio de Interior alemán como un ente especial para tratar de forma específica la protección de datos de carácter personal.
[350] En Francia actúa como entidad de control el CNIL (www.cnil.fr), en Italia existe como institución que se dedica a la vigilancia del cumplimiento de la protección de datos el Garante per la protezione dei dati personali (http://www.garanteprivacy.it/), y en Portugal asume esa inspección la Comissao Nacional de Protecçao de Datos (http://www.cnpd.pt/).
[351] BOE núm. 245 de 11 de octubre de 2011.
[352] Art. 177 de la LJS; "*Cualquier trabajador o sindicato que, invocando un derecho o interés legítimo, considere lesionados los derechos de libertad sindical, huelga u otros derechos fundamentales y libertades públicas, incluida la prohibición de tratamiento discriminatorio y del acoso, podrá recabar su tutela a través de este procedimiento cuando la pretensión se suscite en el ámbito de las relaciones jurídicas atribuidas al conocimiento del orden jurisdiccional social o en conexión directa con las mismas, incluidas las que se formulen contra terceros vinculados al empresario por cualquier título, cuando la vulneración alegada tenga conexión directa con la prestación de servicios".*
[353] BAJO GARCÍA, I.: La tutela judicial de los derechos fundamentales y libertades públicas, Boletín Laboral núm., 2013 disponible en http://www.elderecho.com /tribuna/laboral/ derechos _fundamentales_de_los_trabajadores-libertades_publicas_en_el_Orden_Social-leyreguladora _de_la_Jurisdiccion_Social-libertad_sindical_11_594430003.html. [Consulta 20/01/2015]; BLASCO JOVER, C.: "Las novedades introducidas en la modalidad procesal de tutela de derechos fundamentales tras la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social", *Actualidad Laboral,* núm. 15-16, 2012, pág. 1.

País Vasco cuentan con su propia Agencia de Protección de Datos con competencia en cada uno de estos territorios. Al igual que ocurría en la Comunidad de Madrid que ha tenido su propia Agencia de Protección de Datos hasta que fue suprimida por la Ley 8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas de la Comunidad de Madrid[354]. Por su parte, la Comunidad Autónoma de Andalucía ha hecho una apuesta por la gestión y control de los datos en su ámbito territorial con la creación del Consejo de Transparencia y Protección de datos.

Esta descentralización de los órganos de inspección y vigilancia ya se contemplaba en la LORTAD puesto que preveía la creación de órganos de control tanto en las Comunidades Autónomas como en la Administración Local, si bien la LOPD ha eliminado estos órganos locales de vigilancia, ampliando el ámbito de actuación de las instituciones de control de las Comunidades Autónomas con el objetivo de que un mismo organismo control también los ficheros creados y gestionados por la Administración Local. Sin embargo, estas agencias de control autonómicas no podrán hacerse cargo de los ficheros privados, tal y como ratificó la Sentencia del Tribunal Constitucional, de 30 de noviembre de 2000[355].

Por tanto, el sentido de la creación de las agencias autonómicas de protección de datos es proporcionar al ciudadano más cercanía a la hora de efectuar las reclamaciones pertinentes, si encuentra que se ha infringido su

[354] Boletín Oficial de la Comunidad de Madrid de 29 de diciembre de 2012.
[355] RTC 2000\290; "*La Generalidad de Cataluña en su recurso reivindica, en consecuencia, la competencia de las Comunidades Autónomas para el ejercicio de las potestades y funciones de tutela sobre aquellos ficheros de titularidad privada creados por particulares en la consecución de actividades sobre las que la Comunidad Autónoma puede ostentar títulos* competenciales*, y sobre los creados por la Administración Local de Cataluña, considerando contraria a la Constitución la reserva de tales competencias con carácter exclusivo a la Agencia de Protección de Datos creada por la citada e impugnada Ley Orgánica. Dice la Generalidad de Cataluña que la LORTAD no se ha limitado a imponer restricciones al uso de la informática y definir los correspondientes derechos de la persona al respecto, sino que además ha arbitrado una serie de mecanismos de defensa jurídica de los individuos frente al uso extralimitado de la informática, creando un órgano especializado al que le encomienda en exclusiva la función de verificar la correcta aplicación de la LORTAD. Esta Ley ha reconocido a las Comunidades Autónomas competencias únicamente para el control sobre los ficheros creados por su propia Administración, reservando en exclusiva la tutela administrativa de los ficheros de titularidad privada y los creados por la Administración Local a la Agencia de Protección de Datos, órgano de naturaleza estatal".*

derecho a la protección de datos[356]. Otro de los motivos para la instauración de las agencias autonómicas puede ser el relacionado con la necesidad de auxiliar a la AEPD, sobre todo debido a la ampliación competencial experimentada en el año 2003 en relación con las materias de inscripción de registros, sancionadora y de inspección. Ahora bien, la creación de estas agencias se tiene que hacer respetando siempre dos límites importantes: por un lado, la Comunidad Autónoma no podrá legislar sobre el establecimiento de condiciones básicas de lo que se pueda derivar que el derecho a la protección de datos de carácter personal no es igual para todos los ciudadanos españoles; y, por otra parte, una Comunidad Autónoma no puede regular aspectos de un derecho fundamental si esto no está contemplado en su Estatuto de Autonomía[357].

5.1. La Agencia Española de Protección de Datos.

Como se ha dicho repetidamente, la protección de los datos de carácter personal está controlada en España por la AEPD, creada para cumplir con el mandato de la Disposición final primera de la LORTAD, configurándose como un ente de derecho público con personalidad jurídica propia que actúa con plena independencia en el ejercicio de sus funciones[358]. La aprobación de su Estatuto vino dada por el RD 428/1993, de 26 de marzo[359], adelantándose, de esta forma, a lo que posteriormente estableció el art. 28 de la Directiva 95/46/CE, en el que se preveía la creación de una autoridad de control para vigilar el cumplimiento de la normativa sobre protección de datos. Su denominación ha sido modificada por lo establecido en el art. 79 de la Ley 62/2003, de medidas fiscales, administrativas y de orden social[360] en el que se señalaba que a partir del 1 de enero de 1994, dicha autoridad pasaría a

[356] También el TC justifica la descentralización de la administración pública alegando que con ella se posibilita el ejercicio inmediato de las actuaciones que se tengan que realizar ante los entes administrativos correspondientes, vid., Sentencia del Tribunal Constitucional 25/1983 de 7 de abril de 1983 (RTC 1983/25), FJ 3.
[357] MARZO PORTERO, A.: "La Agencia Española de Protección de Datos" en ALMUZARA ALMAIDA, C. (coord.) *Estudio práctico sobre la protección…,* op. cit., pp. 563-564.
[358] En la actual LOPD, la AEPD queda definida en el art. 35 como: "*un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno".*
[359] BOE núm.106 de 4 de mayo de 1993.
[360] BOE núm. 313 de 31 de diciembre de 2003.

llamarse Agencia Española de Protección de Datos, con la finalidad principal de no confundir esta Agencia con las existentes en las Comunidades Autónomas.

La creación de la AEPD se hacía necesaria, pues era conveniente que existiera una autoridad administrativa que controlara el cumplimiento de la normativa sobre protección de datos. A pesar de la supervisión que realiza la AEPD respecto de la licitud en el tratamiento de datos[361], el titular de los datos de carácter personal podrá dirigirse a la vía judicial[362]. Lógicamente, se puede acudir a los Tribunales si la resolución dada por la AEPD al supuesto concreto no ha respondido a las expectativas del titular de los datos, o, incluso, si el ciudadano lo estima oportuno, se podría acudir directamente a la vía judicial sin haber presentado previamente queja o reclamación ante el organismo administrativo (AEPD).

El régimen jurídico de la AEPD lo dispuesto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común[363] respecto al ejercicio de sus competencias al tratarse de un órgano administrativo[364]; también se le

[361] El procedimiento puede comenzar a través de un sistema de denuncias con el siguiente contenido: Se le informa que, si dispone de pruebas o indicios que puedan acreditar que un hecho pueda suponer el incumplimiento de la Ley Orgánica de Protección de Datos (LOPD), y que pueda constituir una infracción administrativa, puede presentar una denuncia poniendo en conocimiento de esta Agencia la existencia de esos hechos: El escrito de denuncia deberá contener los siguientes elementos esenciales: a) Nombre y apellidos del interesado y en su caso, de la persona que lo presente, así como la identificación del medio preferente o del lugar que se señale a efectos de notificaciones .b) Hechos, razones y petición en que se concrete, con toda claridad, la solicitud. c) Lugar y fecha. d) Firma del solicitante o acreditación de la autenticidad de su voluntad expresada por cualquier medio. e) Órgano, centro o unidad administrativa a la que se dirige. f) Identificación de los presuntos responsables. g) Todos aquellos documentos o cualquier otro tipo de prueba o indicio que permita corroborar los hechos denunciados. Si desea presentar una denuncia, en la sede electrónica de la AEPD dispone de un formulario electrónico que, una vez cumplimentado podrá presentarlo bien en el registro electrónico, si dispone de un certificado de firma, o bien podrá imprimirlo y presentarlo en el registro de documentos de la AEPD situado en la C/ Jorge Juan, 6, 28001-Madrid. Disponibleen:https://www.agpd.Es/portalwebAGPD/CanalDelCiudadano/denunciasciudadano/index-ides-idphp.php) [Consulta 13/02/2015].

[362] En algunos países no se da la opción de acudir previamente a la vía administrativa, sino que directamente la potestad sancionadora referida al incumplimiento de la LOPD la ostenta el poder judicial. Es el caso de Francia, tal y como expone el art.41 de la Loi nº78-17 du 6 janvier 1978 relative á l'informatique, aux fichiers et aux libertés; en Gran Bretaña los ciudadanos que observen cualquier infracción de su derecho a la protección de datos, acudirán a la vía judicial (art. 19 de la Data Protection Act).

[363] BOE núm.285 de 27 de noviembre de 1992.

[364] Vid., art. 12 Ley 30/1992.

aplicarán algunos preceptos de la Ley presupuestaria que establecen normas generales relativas a las agencias estatales, su organización y funcionamiento[365], si bien en lo que se refiere a adquisiciones patrimoniales y a la contratación, la Agencia está sujeta al derecho privado. Pese a su carácter independiente, la AEPD no goza de un patrimonio propio para el ejercicio de sus actividades sino que elabora con carácter anual un anteproyecto de presupuesto y lo remite al Gobierno para que sea integrado en los Presupuestos Generales del Estado.

La AEPD ostenta muchas funciones[366] con la finalidad general de velar por el cumplimiento de la normativa sobre protección de datos de carácter personal, siendo las más destacadas y la que más influencia tienen a la hora de controlar el tratamiento de datos de los trabajadores las referidas a: atender a las peticiones y reclamaciones de los afectados; promover campañas de difusión a través de los medios; ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos; autorizar las transferencias internacionales de datos; dictar instrucciones y recomendaciones de adecuación de los tratamientos a la LOPD[367]; dictar recomendaciones en materia de seguridad y control de acceso a los ficheros; y, finalmente, tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.

[365] Véase art. 21.3, art. 34.1 c) y Disposición Adicional Nonagésimo Tercera de la Ley 36/2014, de 26 de diciembre, de Presupuestos Generales del Estado para el año 2015 (BOE núm.315 de 30 de diciembre).
[366] Vid. art. 37 de la LOPD.
[367] En el ámbito laboral existen, entre otros, algunos informes jurídicos que pueden orientar o solucionar algunos casos que se pueden plantear: Informe jurídico 0184/2013 sobre Red social y creación de perfiles de empleados, disponible en https://www.agpd.es/portalwebAGPD /canaldocumentacion/informes_juridicos/common/pdf_destacados/2013-0184_Red-social-y-creaci-oo-n-de-perfiles-de-empleados..pdf. [Consulta 22/02/2015]; Informe jurídico 0077/2013 sobre captación de imágenes de empleados públicos, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdf_destacados/2013-0077_Captaci-oo-n-y-grabaci-oo-n-de-im-aa-genes-de-empleados-p-uu-blicos .pdf.[Consulta 22/02/2015]; Informe jurídico 0176/2012 sobre recepción de llamadas en teléfono corporativo, disponible en http://www.agpd.es/portalwebAGPD/ canaldocumentacion/informes_juridicos/common/pdf_destacados/2012-0176_Cesi-oo-n-de-listado-de-llamadas-recibidas-en-tel-ee-fono-corporativo..pdf. [Consulta 22/02/2015];

Para el cumplimiento de estas funciones la AEPD se organiza siguiendo las indicaciones del art. 11 del Estatuto de la Agencia Española de Protección de Datos[368]. En este sentido, se establece como órgano ejecutivo de la AEPD el Director, del que dependen jerárquicamente el Registro General de Protección de Datos, la Inspección de Datos y la Secretaría general. También se configura dentro de los órganos de la AEPD el Consejo Consultivo[369] que realiza labores de asesoramiento y que tiene como particularidad que se compone de miembros de procedencia muy dispar con el objetivo de promover la presencia de personas con distintas inquietudes sociales[370].

Los miembros del Consejo Consultivo son nombrados y cesados por el Gobierno, y la duración de su mandato, al igual que ocurre con el cargo de Director de la Agencia, es de cuatro años. El Consejo Consultivo se rige por lo establecido en el Capítulo II del Título II de la Ley 30/1992 adoptando sus acuerdos en sesión plenaria y actuando como presidente de la sesión el Director de la AEPD, y como secretario con voz y sin voto, el que lo sea de la AEPD. Las reuniones se realizan cuando así lo decida el Director de la Agencia, estando previsto que se convoquen cada seis meses o, en todo caso, cuando lo soliciten la mayoría de los miembros del Consejo[371].

---

[368] Art.11 del Estatuto de la AEPD: "*La Agencia de Protección de Datos se estructura en los siguientes órganos: 1. El Director de la Agencia de Protección de Datos.2. El Consejo Consultivo.3. El Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General, como órganos jerárquicamente dependientes del Director de la Agencia."*

[369] De este modo, forman el Consejo Consultivo de la AEPD según el art. 38 de la LOPD: un diputado propuesto por el Congreso de los Diputados, un senador propuesto por el Senado; un representante de la Administración General del Estado y otro de la administración local., un miembro de la Real Academia de la Historia; un experto en la materia; un representante de los usuarios y los consumidores; un representante de cada Comunidad Autónoma; y un representante del sector de ficheros privados, propuesto por el Consejo Superior de Cámaras de Comercio, Industria y Navegación (art. 19.1 i) del RD 428/1993).

[370] Sobre el régimen jurídico de la AEPD vid.: TERRADO SÁNCHEZ, F.: "La agencia de protección de datos: regulación orgánica y estatutaria" *Actualidad Informática Aranzadi*, núm.9, 1993; TÉLLEZ AGUILERA, A.: *Nuevas tecnologías, intimidad*…, op. cit., pp. 212-218; LÓPEZ RAMÓN, F.: *La Agencia de protección de datos como Administración independiente* en Jornadas sobre protección de datos, AEPD, 1996, pp. 255-260.

[371] MURILLO DE LA CUEVA, P.L: *Informática y…,* op. cit. pp. 121-140; VELEIRO REBOREDO, B: *Protección de datos de carácter personal…,* op. cit, pp. 175-183; VV.AA: *Introducción a la Protección de datos,* Dykinson*,* 2006*,* pp. 109-116; CANALES GIL, A: "La agencia española de protección de datos" en VV.AA: *Protección de datos de carácter personal en Iberoamérica: (II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala, 2-6 de junio de 2003)*, Tirant lo Blanch, 2005. pp. 289-306; MARZO PORTERA, A.: "La Agencia Española…", op. cit., pp. 566-574.

5.2. Descentralización de la protección de datos de carácter personal: Las agencias autonómicas de control de la protección de datos de carácter personal.

La actividad legislativa y ejecutiva de las Comunidades Autónomas, en lo que al derecho a la protección de datos de carácter personal se refiere, tiene que respetar la distribución de competencia que la Constitución Española establece entre el Estado y las Comunidades Autónomas (art. 148 y 149 de la CE). El reconocimiento por la jurisprudencia, como se ha visto, de un derecho fundamental a la protección de datos de carácter personal vinculado a lo establecido en el art. 18.4 CE afecta al reparto competencial en este ámbito ya que los elementos esenciales de este derecho tienen que ser regulados por Ley Orgánica para la que tan sólo tiene competencia el legislador estatal[372] y, por tanto, las Comunidades Autónomas deberán respetar el contenido de estas disposiciones en el ejercicio de sus competencias relacionadas con la organización, en este caso, de sus agencias autonómicas de protección de datos de carácter personal[373].

Puesto que el art. 149.1 CE establece que el Estado tendrá competencia exclusiva sobre la "*regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.", el* legislador autonómico no podrá legislar sobre las condiciones básicas[374] de los derechos fundamentales, entendiendo por éstas los elementos del derecho que guardan una relación

[372] Así lo establece el art. 81 de la CE: "*1. Son Leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución. 2. La aprobación, modificación o derogación de las Leyes orgánicas exigirá mayoría absoluta del Congreso, en una votación final sobre el conjunto del proyecto".*

[373] Art. 148.1 de la CE: "*Las Comunidades Autónomas podrán asumir competencias en las siguientes materias: 1. Organización de sus instituciones de autogobierno".*

[374] En relación al concepto de «bases», *«nuestra doctrina constitucional ha venido sosteniendo que por tales han de entenderse los principios normativos generales que informan u ordenan una determinada materia, constituyendo, en definitiva, el marco o denominador común de necesaria vigencia en el territorio nacional. Lo básico es, de esta forma, lo esencial, lo nuclear, o lo imprescindible de una materia, en aras de una unidad mínima de posiciones jurídicas que delimita lo que es competencia estatal y determina, al tiempo, el punto de partida y el límite a partir del cual puede ejercer la Comunidad Autónoma, en defensa del propio interés general, la competencia asumida en su Estatuto»* (Sentencia núm. 211/2014 de 18 diciembre del TC (RTC 2014\211).

directa e inmediata con él y que son imprescindibles o necesarios para garantizar la posición jurídica fundamental de todos los ciudadanos.

Se puede decir por tanto que el Estado tiene competencia exclusiva en todo lo que concierne a los derechos fundamentales pues asume la regulación de las condiciones básicas de los mismos, pudiendo las Comunidades Autónomas intervenir en la regulación de estos derechos siempre que cuenten con competencia legislativa en la materia y no interfieran en el tratamiento de las citadas condiciones básicas. Siguiendo este planteamiento, se puede concluir que las Comunidades Autónomas podrán tener competencias relativas al control y gestión de estos derechos, pero no las referidas a la promulgación de normas que versen sobre la regulación de la protección de datos de carácter personal[375].

No toda la LOPD tiene el carácter de Ley Orgánica ya que existen algunos aspectos que no tratan el desarrollo del derecho fundamental a la protección de datos de carácter personal porque regulan otras materias conexas que tienen la naturaleza de Ley Ordinaria. Así la propia Disposición Final Segunda de la LOPD señala como preceptos con carácter de Ley Ordinaria los del Título IV, que trata sobre las disposiciones sectoriales y la creación de ficheros de titularidad pública o privada; los del Título VI, el cual define la Agencia Española de Protección de Datos, las potestades de inspección y los órganos autonómicos; los del Título VII, que versan sobre las infracciones y sanciones; y lo mismo establece, también, para la Disposición Adicional Cuarta, la Disposición Transitoria Primera y la Final Primera[376].

---

[375] Art. 41.1 de la LOPD: "*1. Las funciones de la Agencia de Protección de Datos reguladas en el art. 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los art.s 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido".*

[376] Disp. Adic. 4ª: "*El apartado cuarto del art. 112 de la Ley General Tributaria pasa a tener la siguiente redacción: 4. La cesión de aquellos datos de carácter personal, objeto de tratamiento, que se debe efectuar a la Administración tributaria conforme a lo dispuesto en el art. 111, en los apartados anteriores de este art. o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito tampoco será de aplicación lo que respecto a las Administraciones públicas establece el apartado 1 del art. 21 de la Ley Orgánica de Protección*

Teniendo en cuenta estas limitaciones, algunas Comunidades Autónomas han creado agencias de control para salvaguardar el derecho a la protección de datos en su ámbito territorial de actuación con las mismas funciones que tiene la AEPD, a excepción de lo relativo al movimiento internacional de datos y a la publicidad periódica respecto a la existencia de ficheros. Actualmente existen en España tres agencias autonómicas[377]: la Agencia Catalana de Protección de Datos, la Agencia Vasca de Protección de y el Consejo de Transparencia y Protección de Datos de Andalucía[378].

La Autoridad Catalana de Protección de Datos[379] fue creada por la Ley 5/2002, de la Agencia Catalana de Protección de Datos[380] como organismo independiente que tiene por objeto garantizar, en el ámbito de las competencias de la Generalidad, los derechos a la protección de datos de carácter personal y de acceso a la información vinculada a ellos. Desde este organismo se informa sobre cuáles son los derechos en esta materia, cómo se ejercen y qué hay que hacer en caso de que no sean respetados; también se informa y se asesora sobre las obligaciones que prevé la legislación y se

---

de Datos de carácter personal".; Disp. Trans. 1ª: *"La Agencia de Protección de Datos será el organismo competente para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal respecto de los tratamientos establecidos en cualquier Convenio Internacional del que sea parte España que atribuya a una autoridad nacional de control esta competencia, mientras no se cree una autoridad diferente para este cometido en desarrollo del Convenio"*; Disp. Fin. Primera; "*El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley".*

377 TRONCOSO REIGADO A.: *La protección de datos personales…,* op. cit. pp. 1832-1837.

378 Creado por la Ley 1/2014 de, 24 de junio, de Transparencia Pública de Andalucía (BOJA núm. 124 de 30 de Junio de 2014) y regulado por lo contenido en su Capítulo II. En la actualidad se encuentra elaborado el proyecto de decreto que regula el estatuto del Consejo de Transparencia y Protección de Datos, disponible en http://www.juntadeandalucia.es/export/drupaljda/Version-0-PROYECTO-ET-CTPDA.pdf [Consulta 24/04/2015].

379 Sobre la Agencia Catalana de protección de datos: HERNÁNDEZ I MORENO, J.X.: "La Ley 5/2002, de 19 de abril, de creación de la Agencia Catalana de Protección de Datos." en VV.AA. *Estudios sobre administraciones públicas y protección de datos personales*, AGPDCM, 2006, pp.223-230; MITJANS PERELLÓ, E.: *"*La experiencia de la Agencia Catalana de Protección de Datos*"* en VV.AA. *Estudios sobre comunidades autónomas y protección de datos personales,* AGPDCM, 2006, pp.313-316.

380 BOE núm. 115 de 14 de mayo de 2002. La Disp. Fin. 1ª de la Ley 5/2002 establece que: "*en el plazo de tres meses a contar desde la entrada en vigor de la presente Ley, el Gobierno distará disposiciones necesarias para la aprobación de un Estatuto de la Agencia Catalana de Protección de Datos*". Este ha sido aprobado por Decreto 48/2003, de 20 de febrero, y fue publicado en DOGC. Diario Oficial de la Generalitat de Catalunya núm. 3835, de 4 de Marzo de 2003.

controla que las entidades las cumplan[381]. Sigue el modelo de su homónima de la Comunidad de Madrid pero introduce algunas variaciones entre las que se pueden destacar la obligación de que la Memoria anual se presente ante el Parlamento y se remita al Gobierno autonómico, al Sindic de Greuges[382] y al Director/a de la AEPD.

Para el funcionamiento de la agencia es necesaria la presencia del Director/a de la Agencia y del Consejo Asesor de Protección de Datos de Cataluña, el cual tiene las funciones de asesoramiento, consulta, fijación de criterios y estudio, de acuerdo con lo que se determine por vía reglamentaria. En este sentido, el Director tiene las mismas funciones que el de la Agencia de Protección de Datos de la Comunidad de Madrid, y también su nombramiento se realiza de la misma forma. El Director está asesorado por el Consejo Asesor de Protección de Datos en el cual están representados distintos entes sociales para de esta forma llegar a resoluciones más consensuadas y que así se tengan en cuenta con distintos puntos de vista[383].

La Agencia Vasca de Protección de Datos, cuando ejerce potestades administrativas, sujeta su actividad a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento

[381] Alguno de los informes jurídicos más relevantes, aplicables al entorno laboral, versan sobre: Informe jurídico 54/2014 sobre la cesión a la Generalidad de Cataluña de la nómina de los trabajadores de Ayuntamiento que participan en programas subvencionados; Informe jurídico 29/2009 sobre Comunicación al Comité de Empresa de una empresa pública de datos de los candidatos de la bolsa de trabajo; Informe jurídico 16/2005 sobre Acceso del comité de empresa a datos de los candidatos a los procesos de selección internos, disponibles en http://www.apd.cat/es/llistaDictamens.com.

[382] Traducción literal al castellano: El defensor de las personas.

[383] Tres vocales designados por el Parlamento, por una mayoría de dos tercios al inicio de cada legislatura; tres representantes de la Administración de la Generalidad, designados por el Gobierno; dos representantes de la Administración local de Cataluña, propuestos por las entidades asociativas de entes locales; una persona experta en el ámbito de los derechos fundamentales, propuesta por el Consejo Interuniversitario de Cataluña; una persona experta en informática, propuesta por el Consejo Interuniversitario de Cataluña; un vocal en representación del Instituto de Estudios Catalanes; un vocal en representación de los consumidores y usuarios, propuesto por las organizaciones de consumidores más representativas; el director o directora del Instituto de Estadística de Cataluña. Para el cumplimiento de las funciones que la ley le asigna, y dentro de su ámbito de actuación, corresponden a la Autoridad Catalana de Protección de Datos las competencias de registro, control, inspección, sanción y resolución, así como la aprobación de propuestas, recomendaciones e instrucciones. En lo que a las funciones se refiere, la Agencia Catalana de Protección de Datos tendrá que atender a lo establecido para el Sindic de Greuges para no interferir en las que sean normativamente otorgadas a esta institución.

Administrativo Común. En el resto de su actividad se somete a lo dispuesto en la LOPD y en la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos[384] y en las disposiciones de desarrollo de las mismas. En materia de adquisiciones patrimoniales y contratación, la Agencia Vasca de Protección de Datos está sujeta al derecho público. Sus bienes y derechos pertenecen al patrimonio de la Comunidad Autónoma del País Vasco.

Los órganos de la Agencia Vasca de Protección de Datos son: un órgano unipersonal compuesto por el Director/a nombrado por el Consejo de Gobierno y un órgano colegiado formado por el Consejo Consultivo, en los términos previstos en el art. 16 de la Ley 2/2004[385] . En cuanto a sus funciones se puede decir que son idénticas a las de los órganos ya analizados, si bien, como en el caso anterior, estas actividades de control que realiza la Agencia tendrán que realizarse sin perjuicio de las competencias que tenga atribuidas el Ararteko (Defensor del Pueblo Vasco) y la AEPD. La característica más destacable de la ley creadora de esta agencia autonómica es el establecimiento de un título específico para el régimen de sanciones que sigue el mismo criterio establecido en la LOPD.[386]

Por último el Consejo de Transparencia y Protección de Datos de Andalucía[387], es la autoridad pública independiente, imparcial y de control en

[384] BOE núm. 279 de 19 de noviembre de 2011.
[385] Art. 16 de la Ley 2/2004; "*El director de la Agencia Vasca de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros: un representante del Parlamento Vasco, designado por éste; un representante de la Administración de la Comunidad Autónoma del País Vasco, designado por el Consejo de Gobierno; un representante de los territorios históricos, designado por éstos de común acuerdo; un representante de las entidades locales del ámbito territorial de la Comunidad Autónoma del País Vasco, designado por la asociación más representativa de las mismas en el citado ámbito territorial; dos expertos, uno en informática y otro en el ámbito de los derechos fundamentales, designados por la Universidad del País Vasco previa consulta a las corporaciones de derecho público de la Comunidad Autónoma del País Vasco".*
[386] VV.AA. *Introducción a la…,* op. cit*.,* pp. 117-124; ENDEMAÑO AROSTEGUI, J.M.: "La Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública de creación de la Agencia Vasca de Protección de Datos", en VV.AA. *Estudios sobre administraciones públicas y protección de datos personales*, AGPDCM, 2006, pp.235-239.
[387] Decreto 434/2015, de 29 de septiembre, por el que se aprueban los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía (BOJA núm. 193 de 2 de octubre de 2015).

materia de transparencia y protección de datos en dicha Comunidad Autónoma. Tiene como fin velar por el cumplimiento de la normativa en materia de transparencia pública, tanto en lo que se refiere a publicidad activa como a la defensa y salvaguarda del derecho de acceso a la información pública, y, en materia de protección de datos, garantizando el ejercicio de los derechos reconocidos en la legislación. Otro dato de interés es que existe la posibilidad para cualquier persona o entidad, pública o privada, de presentar ante el Consejo denuncias sobre el incumplimiento de obligaciones de publicidad activa o de protección de datos con el fin de que se abra un procedimiento que también puede iniciarse de oficio.

El Consejo tiene su sede en Sevilla y se estructura en dos órganos: La Dirección del Consejo y La Comisión Consultiva de Transparencia y Protección de Datos. En este último órgano se prevé que queden representados la Administración de la Junta de Andalucía, el Parlamento de Andalucía, la Oficina del Defensor del Pueblo Andaluz, la Cámara de Cuentas de Andalucía, las Universidades Públicas andaluzas, los consumidores y usuarios, las Administraciones Locales andaluzas y los intereses sociales y económicos. La Dirección aprobará anualmente un Informe sobre la actividad del Consejo que será publicado en su sede electrónica.

CAPÍTULO II: PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LOS PROCESOS DE BÚSQUEDA DE EMPLEO.

Sumario: ***1. AGENCIAS Y ENTIDADES DE INTERMEDIACIÓN LABORAL.*** 1.1. El Sistema Nacional de Empleo. 1.2. Agencias de colocación. 1.3. Agencias de recolocación. 1.4. Empresas de trabajo temporal. ***2. LAS TICS EN LOS PROCESOS DE BÚSQUEDA DE EMPLEO.*** 2.1. Nociones sobre los sistemas de selección 2.0. *2.1.1. Concepto y tipología de redes sociales. 2.1.2. Los buscadores de empleo.* 2.2. Herramientas informáticas que colaboran en los procesos de búsqueda y selección de candidatos. *2.2.1. La informatización de los servicios de intermediación pública. 2.2.2. Instrumentos informáticas que colaboran en los procesos de búsqueda y selección de candidatos.* ***3. TRATAMIENTO Y CESIÓN DE DATOS EN LA SELECCIÓN DE PERSONAL.*** 3.1. Planteamiento general. 3.2. Las distintas formas de captación de datos para la selección de personal. 3.3. Aplicación de los principios de la LOPD al tratamiento de datos realizado por la intermediación laboral. 3.4. Problemas derivados del tratamiento de datos del sistema de selección 2.0. *3.4.1. Pautas de privacidad en el tratamiento de datos en las redes sociales. 3.4.2. Buscadores webs de empleo y protección de datos*. 3.5. Descentralización y cesiones de datos en los procesos de búsqueda de empleo. 3.6. Cumplimiento de la protección de datos por los instrumentos informáticos que colaboran con la intermediación laboral. *3.6.1. Intermediación pública, Tics y datos de carácter personal. 3.6.2. Utilización de programas informáticos y su repercusión en el derecho a la protección de datos.* **4. *EL TRATAMIENTO DE LOS DATOS ESPECIALMENTE PROTEGIDOS EN LOS PROCESOS DE BÚSQUEDA DE EMPLEO.*** 4.1. Tratamientos de datos sobre el estado de salud de los demandantes de empleo. 4.2. Tratamientos de datos ideológicos en los procesos de selección de personal. ***5. TRANSFERENCIA INTERNACIONAL DE DATOS COMO INSTRUMENTO DE INTERMEDIACIÓN LABORAL.***

CAPÍTULO II: PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LOS PROCESOS DE BÚSQUEDA DE EMPLEO.

Lo que se pretende en el presente Capítulo es analizar la problemática del acceso y tratamiento de los datos personales del trabajador en su relación con las entidades, organismos, agencias y procedimientos que actúan o sirven en los procesos de búsqueda de empleo, mientras que lo relativo a esa misma cuestión respecto del trabajador en sentido estricto, esto es, en cuanto trabajador en activo y parte de una relación jurídica laboral, será objeto del Capítulo III del presente trabajo.

En una época de cambios laborales acelerados, materializados en las sucesivas reformas normativas[388], cada vez tienen más importancia los sistemas de intermediación laboral, concebidos como herramientas capaces de mejorar la transparencia y el funcionamiento de los mercados laborales. Por ello, la intermediación laboral, definida en el art. 31 de la Ley de Empleo, puede mostrarse como una pieza clave para ayudar en los procesos de colocación de trabajadores, pues su función principal es gestionar las ofertas de empleo que facilitan aquellos empleadores con necesidad de personal para ponerlas en relación con los demandantes de empleo. Además de la intermediación en el mercado de trabajo, la implantación de las TICs ha propiciado que se avance mucho en los procesos de búsqueda de empleo. En este sentido, y gracias a

[388] Estos cambios han tenido su proyección más directa en las reformas laborales acontecidas en los últimos años (2010-2014): año 2010: Real Decreto-ley 10/2010, de 16 de junio, de medidas urgentes para la reforma del mercado laboral (BOE núm.147 de 17 de junio de 2010) y por la Ley 35/2010, de 17 de septiembre, de medidas urgentes para la reforma del mercado de trabajo (BOE núm.227 de 18 de septiembre de 2010); año 2011: RDL 10/2011 de 26 de agosto, de medidas urgentes para la promoción del empleo de los jóvenes, el fomento de la estabilidad en el empleo y el mantenimiento del programa de recualificación profesional de las personas que agoten su protección por desempleo (BOE núm. 208 de 30 de agosto de 2011) y RDL 7/2011 de 10 de junio, de medidas urgentes para la reforma de la negociación colectiva (BOE núm.139 de 11 de junio de 2011); año 2012: Real Decreto-Ley 3/2012, de medidas urgentes para la reforma del mercado laboral (BOE núm.36 de 11 de febrero de 2012); año 2013; Ley 14/2013, de 27 de septiembre, de apoyo a los emprendedores y su internacionalización (BOE núm. 233 de 28 de septiembre de 2013) Real Decreto-Ley 16/2013, de medidas para favorecer la contratación estable y mejorar la empleabilidad de los trabajadores (BOE núm. 305 de 21 de diciembre de 2013); año 2014:Real Decreto-ley 3/2014, de 28 de Febrero, de medidas urgentes para el fomento del empleo y la contratación indefinida (BOE núm. 52 de 1 de marzo de 2014), Ley 1/2014, de 28 de Febrero, para la protección de los trabajadores a tiempo parcial y otras medidas urgentes en el orden económico y social (BOE núm. 52 de 1 de marzo de 2014), y Real Decreto-ley 8/2014, de 4 de Julio, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia (BOE núm.163 de 5 de julio de 2014).

las TICs, los intermediadores de empleo pueden acumular de forma más rápida y operativa información del candidato al empleo así como obtener un perfil más preciso del mismo a partir de la puesta en común de todos los datos almacenados.

Con el uso de los medios informáticos en los procedimientos de intermediación laboral se pueden relacionar datos que, de forma aislada, no serían suficientes para aportar una información relevante sobre el candidato al empleo, pero que, debido a sus distintas funcionalidades y a la facilidad que esos medios tienen de poner en común todas esas informaciones parciales, pueden revelar características íntimas y personales del trabajador. En este sentido, y como consecuencia de que los intermediadores laborales, públicos y privados[389] y aquellas empresas que tengan servicios propios de recursos humanos[390] necesitan conocer información tanto de las ofertas de empleo de las empresas como de aquellos sujetos que lo demandan, también pueden utilizar las TICs como mecanismos colaboradores de la búsqueda de empleo pues existen instrumentos informáticos (redes sociales y buscadores de empleo) que se pueden utilizar como vías para la búsqueda activa de trabajadores.

Por este motivo, se ha considerado necesario estudiar, además, algunos de estos medios configurados por las TICS –redes sociales, buscadores de empleo, webs de los propios servicios de intermediación,

[389] Los intermediarios públicos son aquellos organismos de naturaleza pública que colaboran no sólo en la búsqueda de empleo, sino también en la gestión de ofertas formativas adaptadas a los distintos perfiles profesionales de aquellos desempleados que acuden a ellos para encontrar un empleo. Asimismo, se encuentra dentro de esta tipología de intermediación la actuación de las agencias de colocación y recolocación. Por el contrario, configuran la intermediación privada los sujetos que gestionan las distintas ofertas y demandas de empleo, sin necesidad de financiación pública incluyendo, entre otros, a las ETTs que, además tienen la capacidad de contratar a los trabajadores y cederlos a la empresa que solicita su servicio de intermediación.

[390] Sobre la gestión de datos en las empresas con servicios propios de recursos humanos, cabe precisar que tanto la recogida del dato como el tratamiento se realiza de la misma forma que si se acudiera a los servicios de una empresa de intermediación pública o privada. No obstante, se pueden establecer algunas distinciones referidas a la cesión o comunicación de datos, ya que en el caso de que la selección la haga la propia empresa que contrata, esta información formara parte de un fichero cuyo responsable será el propio empresario, sin que sea necesario comunicar datos de los desempleados a otras entidades pues no contratan los servicios externos de ninguna empresa para hacer la labor de selección de trabajadores.

herramientas de almacenamiento de datos, etc.- y observar el grado de cumplimiento de la normativa sobre protección de datos en relación con los ficheros, integrados por los datos que estos servidores recogen a través de internet. Con ello se quiere subrayar que la agilidad y eficacia en la gestión de recursos humanos de la empresa mediante las tecnologías de la información han generado nuevos problemas relacionados con el derecho a la protección de datos. Aunque es cierto que la propia tecnología permite articular mecanismos de defensa para intentar paliar esos ataques (corta fuegos o "firewalls", protocolo P3P, etc.)[391].

Aunque la intermediación constituye una herramienta clave para colocar a los demandantes de empleo, puede ocurrir que las propias empresas presenten directamente en el mercado de trabajo sus necesidades de trabajadores, sin necesidad de acudir a los servicios de intermediación. Para lo cual, también pueden utilizar todas las herramientas que las TICs ponen a su alcance con ese objetivo, para poder ellas mismas almacenar la información de los candidatos y hacer la búsqueda y posterior selección de los más capacitados para el puesto de trabajo que necesitan cubrir[392].

Es obvio que a través de todos estos medios conductores de los procesos de búsqueda de empleo, primero, se accede a los datos de los aspirantes al trabajo para, luego, en ocasiones, tratar esos datos con la finalidad de seleccionar al candidato que mejor se adapte a las exigencias profesionales del puesto, información que se inscribe dentro de lo que la LOPD califica como datos de carácter personal, por lo que su tratamiento puede entrañar riesgos para su protección. De forma que la intervención en los procesos de colocación puede colisionar con el derecho a la protección de datos de los trabajadores puesto que un manejo inadecuado e impropio de los mecanismos para utilizar y tratar los datos personales del demandante de

[391] FERNÁNDEZ RODRÍGUEZ, J: *Secreto e intervención de las comunicaciones en internet*, Thomson Civitas, 2004, pp. 70-75.
[392] En este punto hay que aclarar que el tratamiento de datos que realiza la propia empresa que oferta el empleo es idéntico al que pudiera realizar cualquier empresa de intermediación, con la única diferencia que el fichero de datos permanece en la misma empresa y que esos datos sólo serán cedidos para hacer efectiva la contratación, como se verá en el Capítulo III.

empleo puede atentar contra su dignidad. Por esta razón, debe encontrarse un punto de equilibrio entre las ventajas que tiene el uso de las herramientas disponibles en los procesos de búsqueda de empleo –intermediación laboral y TICS- y la preservación de los derechos y libertades fundamentales de los ciudadanos que buscan un empleo y que exigen una especial regulación protectora de los datos personales que debe regir tanto al inicio como durante todo el proceso de selección.

Estos sujetos involucrados en los procesos de búsqueda de empleo no sólo manejan datos genéricos de los futuros trabajadores, sino que pueden llegar a utilizar, para hacer la selección de personal, datos especialmente protegidos que revelan informaciones relacionadas con la ideología religiosa o sindical, la raza o la salud del trabajador. En este caso, es claro que el intermediador deberá justificar el posible tratamiento de esos datos particulares cuyo conocimiento, en principio, no es necesario para que el candidato desempeñe adecuadamente su actividad en la empresa, a menos que se requiera un determinado perfil en el que sea imprescindible conocer esa información sensible[393].

También es necesario subrayar que la difusión del uso de internet como método para la búsqueda de candidatos a un empleo ha propiciado que los datos de las personas que estén en situación de búsqueda de empleo puedan atravesar fronteras y transferirse de forma electrónica a otros países de la Unión Europea o de fuera de ella. Razón por la cual esta posible transferencia internacional de datos, concebida como un instrumento transnacional de intermediación, igualmente merece ser tenida en cuenta a los efectos que aquí interesan.

[393] En relación con un determinado tipo de datos puede destacarse la legislación portuguesa que establece ciertas limitaciones; concretamente la Ley 12/2005 de 26 de enero, de protección de datos genéticos en la selección y contratación de trabajadores (Diario de la República núm.18 de 26 de enero de 2005), en la que se ha establecido la prohibición al empresario, y por tanto también a los intermediadores, de realizar test genéticos para la selección y posterior contratación de trabajadores, aún mediando el consentimiento de los mismos.

1. AGENCIAS Y ENTIDADES DE INTERMEDIACIÓN LABORAL.

Aceptado que la intermediación laboral es, sin duda, una herramienta necesaria para la mejora general de la empleabilidad, se puede definir con carácter general, de acuerdo con el art. 31 de la Ley de Empleo, como el nexo de unión entre la oferta de empleo de la empresa y la demanda de los ciudadanos que no tienen empleo y lo buscan. Se trata de una definición general que ha de completarse con lo previsto, de forma más prolija y minuciosa, en el art. 6. a) del Convenio núm. 88 de la OIT, relativo a la organización del servicio del empleo[394]. En todo caso, la generalidad del art. 31 de la Ley de Empleo, al no ser tan explícito en la enumeración de las posibles actuaciones constitutivas de intermediación laboral, permite que se puedan realizar más actos de los incluidos en el Convenio 88 OIT que no puede considerarse que tenga a estos efectos una función limitativa.

Para la realización de todas estas actuaciones se necesitan los servicios de los denominados agentes de intermediación que son los definidos en el art. 32 de la Ley de Empleo[395], el cual, aunque sólo hace referencia de forma clara a los instrumentos de intermediación pública permite deducir, de la propia definición, la inclusión también de los de naturaleza privada, pese a no estar

[394] Convenio núm. 88, de 17 de julio de 1948 sobre organización del servicio del empleo, adoptado en San Francisco, 31ª reunión CIT (09 julio 1948). Ratificado por España el 14 de enero de 1960 (BOE núm. 9, de 11 de enero de 1961. Art. 6. a): "*El servicio del empleo deberá estar organizado de suerte que garantice la eficacia de la contratación y de la colocación de los trabajadores, y a estos efectos deberá: (a) ayudar a los trabajadores a encontrar un empleo conveniente, y a los empleadores a contratar trabajadores apropiados a las necesidades de las empresas, y más especialmente deberá, de conformidad con las reglas formuladas de acuerdo con un plan nacional: (i) llevar un registro de las personas que soliciten empleo; tomar nota de sus aptitudes profesionales, de su experiencia y de sus deseos; interrogarlas a los efectos de su empleo; evaluar, si fuere necesario, sus aptitudes físicas y profesionales, y ayudarlas a obtener, cuando fuere oportuno, los medios necesarios para su orientación o readaptación profesionales; (ii) obtener de los empleadores una información detallada de los empleos vacantes que hayan notificado al servicio, y de las condiciones que deban cumplir los trabajadores solicitados para ocupar estos empleos; (iii) dirigir hacia los empleos vacantes a los candidatos que posean las aptitudes profesionales y físicas exigidas; (iv) organizar la compensación de las ofertas y demandas de empleo de una oficina con otra, cuando la oficina consultada en primer lugar no pueda colocar convenientemente a los candidatos o cubrir adecuadamente las vacantes, o cuando otras circunstancias lo justifiquen".*

[395] Art. 21 Ley de Empleo: *"A efectos del Sistema Nacional de Empleo, la intermediación en el mercado de trabajo se realizará a través de: Los servicios públicos de empleo. b) Las agencias de colocación. c) Aquellos otros servicios que reglamentariamente se determinen para los trabajadores en el exterior".*

expresamente contemplados. De hecho, la aceptación de uno de estos mecanismos de naturaleza privada se materializó formalmente mediante la reforma de la Ley de Empleo[396] introducida por el RDL 3/2012, de 10 de febrero, de medidas urgentes para la reforma del mercado laboral[397], donde se reconocía a las empresas de trabajo temporal la posibilidad de actuar como agencias de colocación. Por otra parte, y al margen de las ETTs, existen otros mecanismos nacidos gracias a la implantación de las TICS –redes sociales, y buscadores de empleo por internet- que se pueden considerar de gestión privada y que colaboran con las agencias de intermediación.

Como consecuencia de la proliferación de cualquiera de estas modalidades empresariales al servicio de la intermediación, muchas veces de naturaleza privada[398], cada vez es más frecuente que el empresario contrate sus servicios con la finalidad de realizar una selección y clasificación de los trabajadores que buscan empleo para comprobar si cumplen las características requeridas por el puesto ofertado. De entre todas las entidades que ofrecen

[396] Art. 33.2 de la Ley de Empleo: *"Las personas físicas o jurídicas, incluidas las empresas de trabajo temporal, que deseen actuar como agencias de colocación deberán presentar con carácter previo una declaración responsable. Esta declaración responsable se presentará ante el Servicio Público de Empleo Estatal en el supuesto de que la agencia pretenda realizar su actividad desde centros de trabajo establecidos en dos o más comunidades autónomas o utilizando exclusivamente medios electrónicos o por el equivalente de la comunidad autónoma, en el caso de que la agencia pretenda desarrollar su actividad desde centros de trabajo establecidos únicamente en el territorio de esa comunidad."* Art. 33.6 de la Ley de Empleo: *"Las empresas de trabajo temporal podrán actuar como agencias de colocación si se ajustan a lo establecido respecto de dichas agencias en esta ley y sus disposiciones de desarrollo, incluida la obligación de garantizar a los trabajadores la gratuidad por la prestación de servicios".*

[397] *Disposición transitoria primera* del RDL 3/2012 (BOE núm. 36 de 11 de febrero de 2012*.): "1. Las empresas de trabajo temporal que en la fecha de entrada en vigor de esta norma hubieran sido ya autorizadas administrativamente para el desarrollo de su actividad con carácter definitivo podrán actuar como agencias de colocación siempre que presenten ante el Servicio Público de Empleo competente una declaración responsable de que reúnen los requisitos establecidos en la Ley de Empleo, y su normativa de desarrollo. 2. Las empresas a que se refiere esta disposición harán constar su número de autorización como empresa de trabajo temporal en su publicidad y en sus ofertas de servicios de reclutamiento y selección de trabajadores, colocación, orientación y formación profesional y recolocación, en tanto no les sea facilitado el número de autorización como agencia de colocación.3. En lo no previsto en esta disposición, se aplicará lo dispuesto en la Ley de Empleo, y su normativa de desarrollo.4. Se autoriza a la Ministra de Empleo y Seguridad Social a aprobar las disposiciones que puedan, en su caso, resultar necesarias para la aplicación de lo establecido en esta disposición".*

[398] En Francia, por ejemplo, con la promulgación de la Loi núm. 2005-32, de 18 de enero de 2005, se persigue la consagración de un concepto amplio de servicio público de empleo incorporando nuevos sujetos (agencias privadas de empleo, empresas de trabajo temporal) al círculo de los agentes del servicio público de empleo. Véase sobre este asunto, AUVERGNON, P.: "Acerca de la intermediación en el mercado de trabajo en Francia", *Revista Temas Laborales*, núm. 117, 2012, pp. 63-65.

servicios de selección de trabajadores quizás sean las ETTs las empresas más utilizadas a estos efectos por el empresario, desde que han asumido tras las últimas reformas legales tareas relacionadas con la intermediación[399], dejando a los otros instrumentos más tradicionales (agencias de colocación y servicios de empleo) en un segundo plano[400]. En consecuencia, es conveniente examinar, en primer lugar y brevemente, las funciones y características de cada uno de estos mecanismos de intermediación, públicos y privados, para, en un momento posterior, comprobar, que es lo que aquí interesa, el grado de cumplimiento del derecho a la protección de datos en el desempeño de sus tareas[401].

1.1. El Sistema Nacional de Empleo.

Es la Ley de Empleo la que en el año 2003 crea el Sistema Nacional de Empleo[402]. El SNE ha experimentado muchos cambios desde sus inicios, pero siempre ha actuado como un mecanismo central en relación con las políticas activas y pasivas de empleo, de acuerdo con lo establecido en su Cartera

[399] El servicio público de empleo intermedia (gestiona las necesidades tanto por el lado de la oferta como por el de la demanda, dando como resultado la colocación de un trabajador en un puesto de trabajo) en 2,2 de cada 100 colocaciones realizadas en el conjunto del mercado laboral. En el primer trimestre de 2013 los Servicios Públicos de Empleo (SPE) registraron 67.390 colocaciones, sobre un total de 3.062.460 colocaciones registradas en el mismo periodo. Por otro lado, las Empresas de Trabajo Temporal han gestionado en los tres primeros meses de 2013, un total de 446.059 colocaciones. Esto supone que las ETTs intermedian un 14,6% del total de colocaciones realizadas en dicho periodo. Es decir, estas empresas intermedian 6,6 veces más que el SEPE. Fuente: Informe regional de ASEMPLEO (Asociación de empresarios dedicados a la gestión de los recursos humanos), disponible en http: //www.asempleo.com/servicio/informes/Informe%20Regional_ITR13.pdf [Consulta 26/05/2015].

[400] La jurisprudencia comunitaria ha apoyado el criterio generalizado de la eficacia de las ETTs, tal y como establece la STJCE de 11 de diciembre de 1997 (Asunto C-55/1996 Job centre II) destacando que la actividad de intermediación en el mercado de trabajo tiene naturaleza económica y la atribución de la misma en régimen de monopolio a un servicio público por la legislación de un Estado miembro (se trataba de Italia) no resulta compatible con el derecho comunitario si se prueba que las oficinas no cumplen satisfactoriamente tal función de facilitar las colocaciones. Véase también la STJCE 23 abril 1991 (asunto C-41/90 Höfner), en la que se establece que el monopolio de una oficina pública, en este caso la oficina federal alemana para el empleo, se juzga no conforme a las normas comunitarias de la competencia y por tanto abusivo.

[401] SEMPERE NAVARRO, A.V; *"*La intermediación laboral en el RDL 3/2012" *Aranzadi Doctrinal* núm. 1, 2012, pp. 6-8; DORREGO DE CARLOS, A; *"*La reforma de la intermediación laboral en la Ley 35/2010: perspectiva desde el sector de las ETT", *Diario la Ley* núm. 7488, 2010, pp. 102-105.

[402] Art. 6 de la Ley de Empleo: *"Se entiende por Sistema Nacional de Empleo el conjunto de estructuras, medidas y acciones necesarias para promover y desarrollar la política de empleo. El Sistema Nacional de Empleo está integrado por el Servicio Público de Empleo Estatal y los servicios públicos de empleo de las comunidades autónomas".*

Común de Servicios[403], centrando su actuación en; la orientación profesional; la colocación; el asesoramiento a empresas; la formación y cualificación para el empleo; y el asesoramiento para el autoempleo y el emprendimiento. De tal forma que, para poder realizar este servicio, el SNE necesita colaboración y, por este motivo, se adopta un modelo descentralizado en el que se coordinan los medios y acciones tanto estatales como autonómicas. Por ello, el SNE está compuesto por el Servicio Público de Empleo Estatal y los Servicios Públicos de las Comunidades Autónomas[404].

Las actividades desarrolladas por el SEPE, organismo autónomo de la Administración General del Estado adscrito actualmente al Ministerio de Empleo y Seguridad Social, están encaminadas, entre otras, a la gestión del empleo, el registro público de los contratos, la gestión de subvenciones de empleo a las empresas y la gestión de las prestaciones por desempleo. La primera aproximación del SEPE a los datos de los trabajadores tiene lugar cuando el empresario registra el contrato de trabajo, aunque en este momento no se obtiene tanta información como cuando el trabajador acude al SEPE para solicitar la prestación por desempleo, ya que para ello el desempleado tiene que estar en posesión de una tarjeta como demandante de empleo para cuya obtención tiene que aportar información concerniente a sus aptitudes formativas, profesionales, además de la propiamente identificativa. Con estos datos se conforma el itinerario curricular del desempleado y se le ofrece orientación para la consecución de un empleo por lo que, como se verá, el tratamiento de estos datos debe cumplir las exigencias normativas sobre

[403] Real Decreto 7/2015, de 16 de enero, por el que se aprueba la Cartera Común de Servicios del Sistema Nacional de Empleo (BOE núm.31 de 5 de febrero de 2015). Carta de Servicios del SEPE 2014-2017, disponible en http://www.sepe.es /contenidos/ que_ es_el_sepe/publicaciones/sobre_el_sepe/carta_servicios_2014_2017.html.[Consulta 1/12/2014]

[404] Según lo establecido en el art. 19 de la Ley de Empleo, estos servicios se presentan como los competentes para gestionar todo lo relativo a la intermediación laboral: *"Se entiende por servicio público de empleo de las comunidades autónomas los órganos o entidades de las mismas a los que dichas administraciones encomienden, en sus respectivos ámbitos territoriales, el ejercicio de las funciones necesarias para la gestión de la intermediación laboral, según lo establecido en los artículos del 31 al 35, ambos inclusive, y de las políticas activas de empleo, a las que se refieren los artículos del 36 al 40, ambos inclusive. 2. Los servicios públicos de empleo de las comunidades autónomas diseñarán y establecerán, en el ejercicio de sus competencias, las medidas necesarias para determinar las actuaciones de las entidades que colaboren con ellos en la ejecución y desarrollo de las políticas activas de empleo y la gestión de la intermediación laboral".*

protección de datos, pues lo lógico es que esa información no sólo se ceda al empresario a la hora de contratar a un determinado candidato, sino que también permanezca en los ficheros o bases de datos del SEPE.

En lo que aquí interesa, las competencias referidas a la intermediación laboral la tienen los SE autonómicos, en su respectivo ámbito, permitiendo con ello cumplir de forma más adecuada con los fines del SNE[405]. Con el reparto de los servicios del SNE se quiere incrementar la eficiencia de las políticas activas de empleo y conseguir, a su vez, generar un sistema en el que cada oficina territorial de empleo focalice y estudie las necesidades de empleo de su zona[406]. Para lo cual es claro que cada SE autonómico tendrá que relacionarse con las empresas que oferten empleos y remitirles, una vez obtenido, el perfil profesional del candidato para ver si encaja en ese determinado puesto de trabajo.

Para cumplir sus fines, los servicios de orientación gestionados por los SE autonómicos utilizan diversas vías para captar tanto ofertas como demandas de empleo - incluyendo tanto las informales de "*gente conocida*" como los servidores electrónicos o el registro adecuado en las oficinas de colocación-. Estas vías pueden ayudar a mejorar los sistemas primitivos de reclutamiento (o, en todo caso, los más inmediatos de bolsas electrónicas), contrarrestando las prácticas basadas en la colocación de trabajadores sin que el empresario dé publicidad a las ofertas de empleo que se puedan generar en su centro productivo[407].

---

[405] Los fines del Sistema Nacional de Empleo, establecidos en la Ley de Empleo, referentes a la intermediación laboral son, por un lado, ofrecer un servicio de empleo público y gratuito a trabajadores y empresarios que facilite la colocación; y, por otro, proporcionar la información necesaria que permita a los demandantes de empleo encontrar un trabajo y a los empleadores contratar los trabajadores adecuados a sus necesidades, asegurando el principio de igualdad en el acceso de trabajadores y empresarios.

[406] VALDÉS DAL-RÉ, F.: "Cooperación y coordinación entre el Servicio Público Estatal de Empleo y los Servicios Públicos de Empleo Autonómicos", *Revista Temas para el debate,* núm. 245, 2015, pp. 27-30; RODRÍGUEZ-PIÑERO ROYO, M.: *Público y privado en el mercado de trabajo de los 90*, Lección Inaugural Apertura Curso Académico, Universidad de Huelva, 1994, pp. 65-66; CASAS BAAMONDE, M. E. Y PALOMEQUE LÓPEZ, M. C.: "La ruptura del monopolio público de colocación: colocación y fomento del empleo", *Relaciones Laborales*, núm. 6-7, 1994, pp. 236-253.

[407] FERNÁNDEZ GARRIDO, J.: "Los Retos de los Servicios Públicos de Empleo: Una visión externa", *Revista Trabajo*, núm. 24, 2011, pp. 112-115.

A pesar del gran abanico de posibilidades que ofrecen los SE autonómicos para gestionar la intermediación en el mercado de trabajo, parece que todavía no han llegado a desplegar los efectos deseados; quizás debido a la mayor confianza de los empresarios, por los resultados obtenidos,en la intermediación privada, o a la proliferación de internet como vía de búsqueda de candidatos de empleo[408].

No obstante, los SEPE y los SE autonómicos también se están modernizando y actualizando a través de herramientas informáticas que permiten la gestión de los datos de las ofertas y demandas de empleo de forma más ágil y cercana, tanto para los candidatos como para los empresarios que tienen necesidad de mano de obra. En este sentido, los empresarios también pueden acceder a los servicios del SNE inscribiendo y acreditando centros para la impartición de acciones formativas en el ámbito de gestión del SEPE; obteniendo autorización para agencias de colocación de ámbito superior a una Comunidad Autónoma y para aquéllas cuya gestión se realiza exclusivamente por medios electrónicos; realizando de forma más ágil la búsqueda de profesionales a través de la web "Punto de Encuentro"; o contratando a trabajadores extracomunitarios utilizando el Catálogo de Ocupaciones de Difícil Cobertura, etc.

Por último, también el SNE fomenta la búsqueda de empleo en el extranjero y para ello existe un servicio denominado Red EURES de Empleo[409],

[408] Sobre la implicación de los SEPCCA en la intermediación, véase el interesante análisis que hace ALUJAS RUIZ, J.A.: "La eficacia del servicio público de empleo en España. análisis de la intermediación laboral a nivel autonómico", *Tribuna de Economía*, núm. 841, 2008, pp.169-175.

[409] En el ámbito de la EU, la red EURES , tiene por objetivo favorecer el funcionamiento de los mercados de trabajo y satisfacer las necesidades económicas, facilitando la movilidad geográfica transnacional y transfronteriza de los trabajadores y garantizando al mismo tiempo que esta se ejerce en condiciones equitativas y respetando las normas laborables aplicables. Esta Red fue establecida por Decisión 93/569/CEE y sustituida a partir del 1 de enero de 2014 por la Decisión 2012/733/UE, de 26 de noviembre, relativa a la aplicación del Reglamento de Ejecución (UE) n ° 492/2011 del Parlamento Europeo y del Consejo en lo que respecta a la puesta en relación y la compensación de las ofertas y demandas de empleo y el restablecimiento de EURES (DOUE L 328/21 de 28 de noviembre de 2012). Al amparo de esta disposición, se han aprobado una serie de ayudas dirigidas tanto a jóvenes trabajadores como a pequeñas y medianas empresa para favorecer por un lado la asistencia a entrevistas en procesos de selección y/o incorporación a puestos de trabajo en países distintos del de su residencia habitual y por otro a facilitar el acceso y la integración laboral en dichos países (RD

que tiene como objetivo proporcionar servicios de información, asesoramiento y contratación/colocación (búsqueda de empleo) a los trabajadores y empresarios. Cuenta con más de 900 consejeros en toda Europa que suministran la información requerida por los solicitantes de empleo y los empresarios mediante un contacto personal. Se trata de especialistas formados que prestan los tres servicios básicos de EURES de información, orientación y colocación, tanto a los solicitantes de empleo como a los empresarios interesados en el mercado laboral europeo, y han adquirido conocimientos especializados en cuestiones prácticas, jurídicas y administrativas relacionadas con la movilidad a escala nacional y transfronteriza. Estos agentes de EURES trabajan en el marco del servicio público de empleo de cada Estado miembro o de otras organizaciones asociadas en la red EURES[410].

1.2. Agencias de colocación.

La legalización de las agencias privadas de colocación, sin ánimo de lucro, tuvo lugar con la aprobación de la Ley 10/1994, de 19 de mayo, sobre medidas urgentes de fomento de la ocupación[411]. Esta norma permitía la existencia de agencias que no tuvieran ánimo de lucro y que, por tanto, persiguieran la realización de actividades que mejoraran la búsqueda de empleo siempre que esa actividad fuera gratuita para quienes acudieran a ellas. El RD 735/1995, de 5 de mayo, por el que se legalizaron las agencias de colocación sin fines lucrativos y los servicios integrados para el empleo[412], vino a establecer una regulación específica para estas agencias que hasta el momento no tenían ninguna norma que tratara de manera más profunda su régimen jurídico y sus funciones. No obstante, la evolución del mercado de trabajo ha propiciado un nuevo concepto de agencia de colocación[413] en el que se admite la existencia de agencias de colocación con y sin ánimo de lucro así

1674/2012, de 14 diciembre, por el que se establecen las bases reguladoras para la concesión de subvenciones públicas destinadas a la financiación de la acción "Tu primer trabajo EURES" (BOE núm. 301 de 15 de diciembre de 2012). Portal de empleo gestionado por la Dirección General de Empleo, Asuntos Sociales e Igualdad de Oportunidades de la Comisión Europea.

[410] Fuente: https://ec.europa.eu/eures/ [Consulta 27/12/2014].

[411] BOE núm. 122 de 23 de mayo de 1994.

[412] BOE núm.109 de 8 de mayo de 1995.

[413] Con la entrada en vigor del Real Decreto-Ley 10/2010, de 16 de junio, de medidas urgentes para la reforma del mercado de trabajo (BOE núm. 147 de 17 de junio de 2010) se incorpora a la Ley de Empleo el art. 33.

como la posibilidad de que estas actúen de forma autónoma, deberán presentar una declaración responsable ante el SEPE[414].

Esta previsión legal ha encontrado su desarrollo en el RD 1796/2010, de 30 de diciembre, por el que se regulan las agencias de colocación[415], que las define como : "*aquellas entidades públicas o privadas, con o sin ánimo de lucro, que, en coordinación y, en su caso, colaboración con el servicio público de empleo correspondiente, realicen actividades de intermediación laboral que tengan como finalidad proporcionar a las personas trabajadoras un empleo adecuado a sus características y facilitar a los empleadores las personas trabajadoras más apropiadas a sus requerimientos y necesidades*[416]".

Con esta inclusión se ha pretendido mejorar el funcionamiento del mercado de trabajo, completando la actividad que venían desarrollando los SEPE[417]. En todo caso, las actuaciones relacionadas con la intermediación laboral y que pueden generar algún conflicto con el derecho fundamental a la protección de datos de los solicitantes de empleo son, entre otras: la información previa sobre las características del candidato, el tratamiento o

[414] Art. 33.1 de la Ley de Empleo: *"A efectos de lo previsto en esta ley se entenderá por agencias de colocación aquellas entidades públicas o privadas, con o sin ánimo de lucro, que realicen actividades de intermediación laboral de acuerdo con lo establecido en el artículo 31 bien como colaboradores de los Servicios Públicos de Empleo, bien de forma autónoma pero coordinada con los mismos. Asimismo, podrán desarrollar actuaciones relacionadas con la búsqueda de empleo, tales como orientación e información profesional, y con la selección de personal. Las empresas de recolocación son agencias de colocación especializadas en la actividad a que se refiere el artículo 31.2.La actividad de las agencias de colocación se podrá realizar en todo el territorio español".*

[415] BOE núm. 318 de 31 de diciembre de 2010.

[416] Art. 2 del RD 1796/2010, de 30 de diciembre, por el que se regulan las agencias de colocación.

[417] GARCÍA GIL, M.B.: "Mecanismos de intermediación laboral tras la reforma laboral de 2010; principales modificaciones", *Revista Aranzadi Doctrinal*, núm. 11, 2011, pp. 4-8; RODRÍGUEZ–PIÑERO Y BRAVO–FERRER, M.: "El nuevo régimen de las agencias privadas de colocación", *Relaciones Laborales*, núm. 3, 2011, pág. 4; MORENO DE VEGA Y LOMO, F.: "El nuevo régimen jurídico de las agencias de colocación", *Actualidad Laboral,* núm. 18, 2011, pp. 15-17; DOMÍNGUEZ MARTÍN, A.: "Las agencias de colocación (o la privatización del desempleo)", *Lex Nova: La Revista,* núm. 63, 2011, pp. 34-37; GARCÍA NINET, J.I.: "Intermediación laboral y agencias de colocación y de recolocación privadas: comentario al Real Decreto 1796/2010, de 30 de diciembre", *Revista Española de Derecho del Trabajo y Seguridad Social*, núm. 24, 2011, pp. 20-25; VV.AA "La reforma del mercado de trabajo durante la crisis financiera internacional" *Derecho PUCP*, núm. 68, 2012, pp. 102-104; RODRÍGUEZ ESCANCIANO, S.: *La intermediación en el mercado de trabajo: Análisis y propuestas*, Tirant lo Blanch, 2012**,** pp. 358-360; LÁZARO SÁNCHEZ, J.L: "Las agencias de colocación" en VV.AA: *Estudios en torno a la reforma laboral 2012*, Ed. Punto Rojo, 2013, pp. 19-34.

almacenamiento de esos datos personales, su análisis en relación con las características y exigencias del puesto de trabajo[418] ; la selección de los trabajadores y el concierto de una entrevista con los más adecuados. Es justamente en este momento en el que se empiezan a producir los tratamientos de datos de estos desempleados, incluso pudiendo servir esta información de guía para poder dirigir la entrevista de trabajo. Por ello, en el propio RD 1796/2010, se hace ya una aproximación a la obligación de respetar la intimidad en el tratamiento de los datos personales[419].

Puede ocurrir que, para el desarrollo de esta tarea, la agencia de colocación no tenga que llegar tratar la información, pues le sirve un simple acceso a los datos sin que llegue a constituir un tratamiento de los mismos en sentido propio y técnico, ya que, cuando se hace referencia al acceso sin tratamiento, se alude a la facultad de visualizar determinados datos para simplemente sopesar si se van a utilizar o ceder a las empresas que han requerido trabajadores para un concreto puesto de trabajo. Ahora bien, lo habitual es que estas agencias incorporen la información a una base de datos de usuarios la cual le servirá para registrar la información de estos candidatos y poder así seleccionar a los que sean más adecuados o que mejor encajen en las ofertas de empleo de las empresas que contratan los servicios de selección[420].

1.3. Agencias de recolocación.

Son agencias privadas de empleo con ánimo de lucro, que ya tenían presencia y actuaban de forma normalizada en países como Holanda y el Reino Unido, pero que en España no han tenido reconocimiento legal hasta la promulgación de la Ley 35/2010, la cual introdujo el concepto de recolocación. Conforme a lo establecido en la Ley 35/2010 la recolocación se centra en el

[418] Vid., art. 5 j) del RD 1796/2010.
[419] Vid., art. 5 e) del RD 1796/2010.
[420] CARDONA RUBERT M.B.: "Los datos del trabajador en las agencias de colocación: aplicación de la Ley 5/1992, de regulación del tratamiento automatizado de datos de carácter personal en las agencias de colocación", en VVAA.: *Inserción laboral: I Jornadas Andaluzas de Relaciones Laborales*, Universidad de Huelva, 1999, pp. 283-294.

servicio que la empresa presta al trabajador despedido por ella como consecuencia de una reestructuración empresarial. No obstante, la recolocación se presenta como un concepto bastante restringido ya que el legislador tan sólo ha querido tenerlo en cuenta para aquellos trabajadores que provengan de una reestructuración empresarial[421], sin que puedan solicitar estos servicios los trabajadores que se quedan sin empleo por otras circunstancias.

Por tanto, a través este mecanismo, es la empresa la que proporciona a estos trabajadores los medios necesarios para lograr la transición en su carrera profesional, de forma que puedan conseguir, en el menor plazo de tiempo posible, un nuevo trabajo en otra empresa lo más adecuado a su perfil y sus preferencias[422], para lo que la empresa o contrata los servicios de consultores externos, o bien utiliza a trabajadores propios. Además de estas tareas el consultor de outplacement trabaja como asesor de imagen, formación y relaciones públicas del candidato, potenciando sus virtudes y reforzando sus puntos débiles, recibiendo el candidato[423], en forma de seminarios, la formación que necesita para tener éxito en la búsqueda de su nuevo puesto de trabajo[424].

---

[421] Art. 2.2 del RD 1796/2010; *"Las empresas de recolocación son agencias de colocación especializadas en la actividad destinada a la recolocación de las personas trabajadoras que resultaran excedentes en procesos de reestructuración empresarial, cuando aquélla hubiera sido establecida o acordada con las personas trabajadoras o sus representantes en los correspondientes planes sociales o programas de recolocación, y estarán sometidas al régimen legal y reglamentario establecido con carácter general para las agencias de colocación".* Art. 31.2 de la Ley de Empleo; "*También se considerará intermediación laboral la actividad destinada a la recolocación de los trabajadores que resultaran excedentes en procesos de reestructuración empresarial, cuando aquélla hubiera sido establecida o acordada con los trabajadores o sus representantes en los correspondientes planes sociales o programas de recolocación*".

[422] BENAVENTE TORRES, I.: "La Reforma de la Intermediación Laboral por la Ley 35/2010", *Revista Trabajo,* núm. 24, 2011, pp. 201-202; RODRÍGUEZ ESCANCIANO, S: *La intermediación en el mercado…,* op. cit., pág. 382; SÁEZ LARA, C: "Espacio y funciones de las empresas de recolocación" *Revista Temas Laborales,* núm. 107, 2010, pp. 338-339, 355-357; VALDÉS DAL-RE, F.: "La reforma de la intermediación laboral", *Relaciones Laborales*, núm. 21-22, 2010, pp. 129-157; GUERRERO VIZUETE, E.: "El plan de recolocación externa de los trabajadores excedentes: un nuevo instrumento de lucha contra el desempleo" en CABEZA PEREIRO, J. (coord.): *Políticas de empleo*, Aranzadi, 2013, pp. 85-98.

[423] SÁEZ LARA, C.: "Espacio y funciones …", op. cit., pp. 337-343; ZAZGNANEAZIZ: "Las agencias de recolocación y los procesos de outplacement: Como aumentar la empleabilidad de los trabajadores y asesorarles en la búsqueda de trabajo", *Revista Capital Humano*, núm. 268, 2012, pp. 34-39; GARCÍA NINET, J.I.: "Intermediación laboral y agencias de colocación…", op. cit., pp. 16-18.

[424] Sobre este tema, véase: RODRÍGUEZ-PIÑERO ROYO, M.: "Outplacement, head-hunter y otras formas de intervención privada en el mercado de trabajo", en *La reforma del mercado de*

En España, como se ha dicho, la actividad de la recolocación está orientada a paliar el desempleo producido por los expedientes de regulación de empleo, dirigiendo su actividad a la consecución de un empleo para los desempleados con estas características, rompiendo así con el concepto más habitual de usuario de los servicios de intermediación. Lo anterior se debe seguramente al hecho de que la forma de intervención en el mercado de trabajo realizada por las agencias de recolocación no cumple exactamente con las características propias de cualquier servicio de intermediación, ya que lo que se pretende, aunque la Ley de Empleo la haya incluido entre las actividades de intermediación, es proporcionar al trabajador despedido la ayuda necesaria para que encuentre un nuevo empleo pero sin mediar estrictamente entre la empresa que oferta el empleo y el trabajador que lo demanda[425]. En todo caso, las agencias de recolocación, para realizar este cometido, necesitan conocer información personal de los trabajadores y suelen crear al efecto un fichero de datos para poder colaboraren la tarea formativa y preparar a estos trabajadores para que encuentren un trabajo.

1.4. Empresas de trabajo temporal[426].

En España, la regulación de las empresas de trabajo temporal no se produjo hasta la promulgación de la Ley 14/1994, de 1 de junio, de empresas de trabajo temporal[427]. No obstante, el reconocimiento de las ETTs como

---

trabajo y de la seguridad y salud laboral, Universidad de Granada, 1996, pp. 227-246; SÁEZ LARA, C.: "Espacio y funciones…", op. cit., pp. 343-345; ARIAS DOMÍNGUEZ, A.: "El "Outplacement" como método de lucha contra un desempleo muy cualificado" *Anuario de la Facultad de Derecho***,** vol. 23, 2005, pp. 263-278; DE LA CASA QUEMADA, S.: "Las empresas de recolocación (outplacement) y nuevos derechos del trabajador a la prevención del desempleo", *Trabajo: Revista andaluza de relaciones laborales*, núm. 20, 2007, pp. 144-145.

[425] RAMÍREZ MARTÍNEZ, J.M.: "El proceso de colocación: intervencionismo público e iniciativa privada" en ALARCÓN CARACUEL, M.R. (coord.): *La reforma laboral de 1994* , Marcial Pons, 1994, pp. 11-44.

[426] Acerca del concepto y funcionamiento de la ETT vid., PÉREZ DE LOS COBOS ORIHUEL F; "La reforma laboral: un nuevo marco legal para las empresas de trabajo temporal" *Actualidad Laboral* núm.16, La Ley, 2010, pp. 65-69; GOERLICH PESET, J. M.:" Reformas en materia de empleo y de empresas de trabajo temporal" en VV.AA, *La Reforma Laboral en el Real Decreto-Ley 10/2010,* Valencia, Tirant lo Blanch, 2010, pág. 165; RAMOS QUINTANA, M.: "Intermediación laboral y empresas de trabajo temporal en la reforma de 2010: la promoción de la intervención privada en el mercado de trabajo", *Revista Relaciones Laborales,* núm. 2, Sección Doctrina, La Ley 2011, pp. 20-23; VV.AA; *Código de intermediación laboral*, WoltersKluwer España, 2011. pp. 21-61; NÚÑEZ-CORTÉS CONTRERAS, P.: "Algunas medidas para favorecer la empleabilidad en la Reforma Laboral 2012", *Actualidad Laboral*, núm. 19, La Ley, 2012, pp. 1-2.

[427] BOE núm.131 de 2 de junio de 1994.

agencias de colocación no se otorgó, como se ha indicado, hasta la promulgación del RDL 3/2012 ya que, antes de esta reforma, tenían restringido su ámbito de actuación a la actividad de cesión temporal de los trabajadores sin tener ninguna facultad en materia de intermediación laboral[428].

Una vez admitida legalmente su capacidad intermediadora, en la LETT se establece el concepto de empresa de trabajo temporal como, en primer lugar, "*aquélla cuya actividad fundamental consiste en poner a disposición de otra empresa usuaria, con carácter temporal, trabajadores por ella contratados. La contratación de trabajadores para cederlos temporalmente a otra empresa sólo podrá efectuarse a través de empresas de trabajo temporal debidamente autorizadas en los términos previstos en esta Ley.* Añadiendo, en segundo lugar, que: *Las empresas de trabajo temporal podrán, además, actuar como agencias de colocación cuando cumplan los requisitos establecidos en la Ley 56/2003, de 16 de diciembre, de Empleo, y su normativa de desarrollo. En su relación tanto con los trabajadores como con las empresas clientes las empresas de trabajo temporal deberán informar expresamente y en cada caso si su actuación lo es en la condición de empresa de trabajo temporal o de agencia de colocación[429]".* Las ETTs precisan autorización de la autoridad laboral competente para actuar como agencias de colocación siguiendo lo establecido en el art. 2[430] del RD 417/2015, de 29 de mayo, por el que se prueba el Reglamento de Empresas de Trabajo Temporal[431]

Así pues, cuando una empresa necesita cubrir temporalmente un puesto de trabajo y recurre a una ETT, la práctica habitual es redactar un contrato por medio del cual ésta establece una relación mercantil con la empresa usuaria. Es, entonces, cuando la ETT inicia un proceso selectivo que culmina con la

[428] Vid., la concreta descripción de las distintas reformas que afectaron a la configuración de las ETTs como agencias de intermediación que hace VICENTE PALACIO, M.A.: "El Real Decreto-ley 3/2012, de 10 de febrero, de medidas urgentes para la reforma del mercado laboral: una breve presentación de la reforma en el ámbito del derecho individual", *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 31, 2012, pp. 275-277.
[429] Art. 1 de la Ley 14/1994.
[430] Art. 2 del RD 417/2015: *"1. Las personas físicas o jurídicas que pretendan realizar la actividad constitutiva de empresa de trabajo temporal deberán obtener autorización administrativa previa de la autoridad laboral competente. 2. La autorización administrativa será única, tendrá eficacia en todo el territorio nacional y se concederá sin límite de duración".*
[431] BOE núm. 147 de 20 de junio de 2015.

elección, entre los candidatos presentados, del trabajador más idóneo para cubrir ese puesto de trabajo atendiendo a las especificidades ofrecidas por la empresa usuaria y a la experiencia, formación, actitudes y disponibilidades que tiene el candidato. En este momento, además de actuar como agencia de colocación, las ETTs actúan como sujeto contratante para ceder a esos trabajadores a otras empresas, equiparando estas acciones, desde el punto de vista de algunos autores, a las de un empleador o sujeto que forma parte del mercado de trabajo[432].

En la búsqueda de empleo a través de ETTs se produce siempre una triple relación entre la ETT y el trabajador (relación laboral); la que se establece entre la ETT y la empresa usuaria (relación mercantil)[433]; y la existente entre la empresa usuaria y el propio trabajador que es una relación de carácter funcional, pues el trabajador sólo está sometido a la dirección y coordinación del empresario para el desarrollo de sus funciones[434].

---

[432] GALA DURÁN, C.: "La Directiva sobre empresas de trabajo temporal y su impacto en España", *Temas Laborales: Revista Andaluza de Trabajo y Bienestar Social*, núm. 102, 2009, pp. 33-36; MONEREO PÉREZ J.L Y MORENO VIDA, N.: "Las empresas de trabajo temporal en el marco de las nuevas formas de organización empresarial", *Revista Española del Ministerio de Trabajo y Asuntos Sociales*, núm. 48, 2004, pág. 52; RODRÍGUEZ-PIÑERO ROYO, M.: "El nuevo papel de las empresas de trabajo temporal" en VV.AA.: Diez años desde la regularización de las empresas de trabajo temporal, Mergablum (CARL), 2004, pp. 17-20; PÉREZ ESPINOSA, F.: "Las empresas de trabajo temporal: a medio camino entre la apertura de los sistemas de colocación y la flexibilización de la mano de obra" en VV.AA.: *La reforma del mercado laboral*, Lex Nova, 1999, pp. 99 y ss.

[433] Se realiza un contrato de puesta a disposición definido en el art. 6.1 de la Ley 14/1994 de Empresas de Trabajo Temporal; "*El contrato de puesta a disposición es el celebrado entre la empresa de trabajo temporal y la empresa usuaria teniendo por objeto la cesión del trabajador para prestar servicios en la empresa usuaria, a cuyo poder de dirección quedará sometido aquél";* El contenido del contrato de puesta a disposición viene establecido en el art. 14 del RD 417/2015*: "De la información existente en los Registros de Empresas de Trabajo Temporal, los datos que a continuación se relacionan se incorporarán a una base de datos central, cuya gestión corresponderá a la Dirección General de Empleo del Ministerio de Empleo y Seguridad Social: a) Identificación de la empresa; b) Autorización para el desarrollo de la actividad de empresa de trabajo temporal, incluidos los supuestos de reanudación, así como de suspensión o cese de actividades; c) Domicilio social de la empresa y domicilio de los centros de trabajo; d) Cambios de domicilio social de la empresa y aperturas y cierres de centros de trabajo; e) Relaciones de los contratos de puesta a disposición a que se refiere el artículo 17.1. 2. Los datos incluidos en las letras a), b), c) y d) serán de acceso público. 3. Los datos de la letra e) serán accesibles para las autoridades laborales".*

[434] HERNÁNDEZ LAHOZ, M. Y GIL LACRUZ, M.: "Origen y evolución de las empresas de Trabajo Temporal", *Revista Capital Humano*, año nº 24, núm. extra 257, 2011, pp. 26-32; RODRÍGUEZ-PIÑERO ROYO, M.: "Concepto de empresa de trabajo temporal" en VV.AA.: *Comentario a la Ley de Empresas de Trabajo Temporal*, La Ley, 2009, pp.37-76; TENA TENA, G.: "Los pros y los contras de las empresas de trabajo temporal", *Acciones e investigaciones sociales*, núm. 10, 2000, pp. 53-57; GONZÁLEZ ORTEGA, S. Y GÓMEZ-MILLÁN HERENCIA, M.J.: "Forma y duración" en

En lo que al derecho a la protección de datos de carácter personal se refiere se pueden analizar los distintos problemas que puede generar la citada relación triangular, desde una triple perspectiva: por un lado, el tratamiento de datos de los candidatos al empleo (los que se dirigen a la ETT para la búsqueda de un empleo); por otro lado, la utilización de esos datos para su contratación por la ETT[435]; y por último, habrá que precisar la información transmitida al empresario cuando se produce la cesión de trabajadores a la empresa usuaria.

2. LAS TICS EN LOS PROCESOS DE BÚSQUEDA DE EMPLEO.

Para poder precisar el alcance de las TICS en los procesos de búsqueda de empleo es preciso hacer referencia, en primer lugar, a lo que se conoce como selección 2.0[436]. Este sistema tecnológico, sujeto a las disposiciones de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico[437], permite, entre otras funciones, la búsqueda de candidatos a través de redes sociales o de buscadores de empleo, configurándose estas técnicas como otra forma de reclutamiento del personal. En este sentido, se presenta, por un lado, como una alternativa para la selección de personal en las pequeñas y medianas empresas y, por otro, como un medio utilizado también por las propias agencias de intermediación pues su implantación conlleva que se pueda reclutar personal de una forma sencilla y sin realizar una gran inversión económica[438].

VV.AA.: *Las empresas de trabajo temporal: estudio de su régimen jurídico,* Comares, 2014, pp. 117-118.

[435] Sobre este aspecto se incidirá en el Capítulo III cuando se aborde la contratación de los trabajadores y el uso de los datos, ya que la ETT actúa como cualquier otro empresario a la hora de contratar y tendrá, por tanto, que realizar las mismas gestiones para que el contrato de trabajo sea efectivo.

[436] La selección 2.0 es el modelo mediante el cual las empresas y organizaciones divulgan en el mercado de los recursos humanos las necesidades de talentos (empleados) y puestos de trabajo que pretenden cubrir. Con la inclusión de este concepto en los procesos de búsqueda de empleo se intenta atraer a una mayor cantidad de personas adecuadas y competentes para un puesto de trabajo a través de las herramientas de la web 2.0 y la experiencia colaborativa.

[437] BOE núm.166, de 12 de julio, de 2002.

[438] CARRASCO POLAINO, R.: "Las redes sociales en las organizaciones y su aplicación en la comunicación tanto hacia el mercado como hacia sus miembros" en VV.AA.: *Retos empresariales en un nuevo entorno*, Netbliblo, 2010, pág. 61; CELAYA, J.: *La empresa en la web*

En relación con el ahorro empresarial, económico y procedimental que puede suponer la utilización de sistemas de selección 2.0 se observa que la aplicación de estos instrumentos es más eficaz que la publicación de ofertas de empleo en prensa ya que, a través de estos mecanismos, se transmiten a un número más elevado de personas a la vez que se hace posible el análisis, en un tiempo record, de la aptitud del candidato para un determinado puesto de trabajo vacante. La facilidad que proporcionan las TICS, también para los desempleados, se manifiesta en la posibilidad de acceder a la red incluso desde el propio teléfono móvil y consultar las ofertas de empleo publicadas en las redes sociales o a través del llamado boca a boca virtual (los usuarios de internet pueden avisar a otros sobre las posibles ofertas de empleo), para así conocer las posibles vacantes que pueden ofertar las empresas de intermediación laboral.

En segundo lugar, las TICs también se presentan como herramienta colaboradora para potenciar y flexibilizar los procesos de búsqueda de empleo. En este sentido, se puede decir que la alta capacidad que tienen las tecnologías informáticas para almacenar y filtrar datos de carácter personal, también se ha trasladado al ámbito de la búsqueda y selección de candidatos al empleo. Así pues, estos mecanismos de recopilación de información personal son utilizados tanto por las empresas de intermediación públicas y privadas, como por las entidades que realizan su propia selección de personal. Muchos de estos procedimientos, además de ofrecer servicios de registro de datos, se configuran como verdaderas oficinas virtuales de empleo que ofrecen una amplia cartera de servicios para colaborar en la colocación de aquellas personas que estén a la búsqueda de un empleo.

2.1. Nociones sobre los sistemas de selección 2.0.

2.0. El impacto de las redes sociales y las nuevas formas de comunicación online en la estrategia empresarial, Gestión 2000, 2008, pp. 103-105.

2.1.1. Concepto y tipología de redes sociales.

Las redes sociales, concebidas como modelo colaborativo y abierto a la participación de todos los usuarios posibles[439], han supuesto un gran avance en la selección de demandantes de empleo por la agilización y simplificación que pueden suponer para el proceso de selección de personal. La navegación por las citadas redes sociales propicia que el intermediador laboral pueda acceder a, y tratar, una gran cantidad de información sobre las personas que están buscando un empleo, por lo que habrá que analizar si estos sistemas ofrecen la protección suficiente al titular del dato[440].

Las redes sociales[441] tienen una serie de ventajas en lo que a la selección de personal se refiere porque facilitan la interactuación con más de un contacto a la vez para así intentar elegir al mejor candidato[442]. Esta forma de selección puede llegar a convertirse en una tarea de equipo en la que no sólo interviene el personal de recursos humanos sino cualquier trabajador de la empresa que visualice el perfil de un candidato porque previamente se haya

[439] Según datos estadísticos, en 2013 Facebook contaba con 1.100 millones de usuarios activos mensuales en todo el mundo, de los cuales un 23% se conecta a sus cuentas más de 5 veces al día. Twitter había superado a finales de 2012 los 485 millones de usuarios, de los cuales 288 son usuarios activos, mientras Tuenti rebasa los 14 millones de usuarios. Google plus se sitúa en los 500 millones de usuarios y LinkedIn en los 225 millones. Por lo que se refiere a España, el 80% de los internautas usa redes sociales, siendo las principales Facebook (con 17 millones de usuarios únicos en España), Youtube, Twitter (5,6 millones), LinkedIn (2,7 millones) y Tuenti (9,6 millones). Son datos obtenidos de "Estadísticas usuarios redes sociales en España. 2013 (www.concepto.05.com) y "Cifras y estadísticas de las Redes Sociales 2013" (www.rvillanuevarios.com).

[440] MORATO GARCÍA, R.: "El impacto de las redes sociales virtuales en los procesos de selección de trabajadores" Comunicación presentada al X Congreso Europeo de Derecho del Trabajo y de la Seguridad Social, Sevilla, 2011, pp. 10-12, disponible en: http://www.aedtss.com/images/stories/documentos/congresoeuropeocomunicaciones/1/106morato_garcia.pdf). [Consulta 23/12/2014].

[441] Se entiende por red social: *Lugares en Internet donde las personas publican y comparten todo tipo de información, personal y profesional, con terceras personas, conocidos y absolutos desconocidos*. Según Wikipedia; *son estructuras sociales compuestas de grupos de personas, las cuales están conectadas por uno o varios tipos de relaciones, tales como amistad, parentesco, intereses comunes o que comparten conocimientos*. Son muchas las organizaciones que actualmente ignoran o tienen poco conocimiento de las tecnologías sociales, su funcionamiento y las ventajas o beneficios que pueden aportar. Mirar "hacia otro lado" cuando se habla de innovaciones en las tecnologías es una manera de no querer avanzar e introducirse en este mundo tan importante que es el de las nuevas tecnologías, que inevitable y drásticamente cambian la forma personal y laboral de comunicarnos.

[442] Ahora bien siguiendo lo establecido en el art. 5.3 de la Recomendación CM/Rec del Comité de Ministros de la UE sobre el tratamiento de datos personales en el contexto del empleo, de 1 de abril de 2015, los empleadores no podrán conocer la información que comparta ni el candidato al empleo ni el trabajador con otros usuarios.

registrado como usuario en la red social y, por tanto, este trabajador también podrá aportar información a los que se dediquen a la selección de personal. Estas comunicaciones de datos, que pueden llegar a influir en un proceso selectivo, deben ser sin duda respetuosas con los principios de protección de datos y aunque, en principio, estas averiguaciones de información pueden ser beneficiosas para el demandante de empleo, un mal uso de los datos puede provocar perjuicios en la selección de los candidatos más adecuados.

A este respecto, otra de las posibilidades que ofrece la selección de personal a través de las redes sociales profesionales es la de obtener datos de los denominados candidatos pasivos, que son aquellos que pueden encajar perfectamente en el perfil que busca la empresa de intermediación pero que no se encuentran en búsqueda activa de empleo. Con ello, el buscar candidatos a través de las redes sociales ha contribuido a que no sólo se puedan encontrar personas desempleadas disponibles, sino que también que se puedan ofrecer oportunidades de empleo más competitivas y más acordes con sus características formativas y profesionales[443] a aquellos trabajadores que tengan intención de cambiar de empleo.

A pesar del gran número de redes sociales que existen, si lo que se pretende es seleccionar personas para trabajar en una determinada empresa, lo lógico es que se acuda a las redes sociales profesionales, siendo las más utilizadas[444]: LinkedIn, Viadeo, Xing, Ziki.[445].Con estos mecanismos se consigue efectividad a coste cero puesto que la inscripción en la mayoría de redes profesionales para buscar candidatos es gratuita. Aunque si se quiere utilizar la red profesional para realizar alguna tarea concreta (por ejemplo, el diseño específico de un plan de selección; buscar candidatos con filtros de búsqueda avanzada para seleccionar personal; poder indagar perfiles distintos

[443] DE PABLOS, S.: "El impacto 2.0 en la búsqueda y selección de profesionales con talento", *Revista Capital Humano,* núm. 248, 2010, pp.1-3; MAROÑO OTERO, E.: "¿Cómo están afectando las redes sociales al mercado laboral en España?", *Revista Capital Humano*, núm. 287, 2014, pp. 4-5.
[444] Fuente: http://www.redesociales.net/redesprofesionales/.
[445] La misión de estas redes sociales profesionales consiste en poner en contacto a profesionales de todo el mundo para que sean más productivos y tengan más éxito en el ámbito laboral, por lo que se permite que los usuarios puedan acceder a informaciones laborales incluso de otros países.

de los establecidos en la red de contactos etc.), se puede contratar los servicios premium con un coste que no suele ser elevado.

El candidato al empleo se involucra así más en su proceso de selección al interactuar directamente con el seleccionador. Por otro lado, se permite que se acceda, de forma realmente sencilla, a los datos de carácter personal que los usuarios exponen en la red social. Para ello, tan sólo es necesaria una conexión a internet y el registro en una concreta red social profesional para poder reunir o visualizar la información sobre un demandante de empleo que tenga un perfil activo en esa red social.

Sin embargo, es posible que a través de estos sistemas se puedan descubrir aspectos sobre los gustos o actividades del candidato al empleo, vinculados normalmente a su intimidad, sobre todo si se realizan consultas en redes sociales que no son de tipo profesional. En estos supuestos, el usuario interactúa con el resto de inscritos de forma diferente que si se encuentra en una red social profesional puesto que, por la finalidad que ésta tiene de ser una herramienta para la búsqueda de empleo, no se muestran comentarios más informales, ni se utilizan como medio para generar contactos que nada tienen que ver con la consecución de un empleo[446].

Por este motivo es necesario distinguir entre redes sociales generales y profesionales. Así, aunque LinkedIn está considerada la red social que más se ajusta a lo que se conoce como red social profesional[447], hay otras como Facebook que, aunque su finalidad principal es generar contactos sociales, han comenzado recientemente, como consecuencia del desempleo existente, a crear grupos de búsqueda de empleo. No obstante, las notas características de las redes sociales no profesionales no permiten que se pueda acceder a las características profesionales de una persona puesto que, para inscribirse en

[446] ALASTRUEY, R.: *Empleo 2.0*. Editorial UOC, 2009; TELLO DIAZ L; "Intimidad y «extimidad» en las redes sociales. Las demarcaciones éticas de Facebook" *Revista Científica de Educomunicación*, 2013, pp. 206-208.
[447] Unique: "Sobre el uso de las redes sociales y profesionales como fuentes de reclutamiento y selección de personal", *Revista Capital Humano*, núm. 248, 2010, pp. 50-53.

ellas, no es necesario indicar este tipo de datos[448]. Estadísticamente, Estados Unidos sigue siendo el país en dónde el reclutamiento a través de esta vía está más implantado, mientras que en España los directivos de las grandes empresas siguen siendo reacios a participar en las redes sociales como miembros activos[449].

2.1.2. Los buscadores de empleo.

La selección de personal a través de los buscadores de empleo es otro de los mecanismos existentes para captar posibles candidatos a una oferta de trabajo. Sobre este aspecto, y teniendo en cuenta el art. 31 de la Ley de Empleo, puede concluirse que, según la definición de agentes de intermediación, los portales de empleo, efectivamente, se consideran como tales debido, sobre todo debido a que su función principal es la de poner en comunicación a los demandantes de empleo con las entidades o empresas que lo ofrecen.[450]

Las agencias de intermediación se benefician bastante de la utilización de estas técnicas ya que, hoy día, es usual la publicación de ofertas de empleo en su página web[451], pudiendo llegar así a comunicar sus necesidades a todos aquellos demandantes de empleo que visiten con asiduidad su portal web. No obstante, aunque se opte por mecanizar los sistemas de intermediación, hay que tener en cuenta que todavía existe una parte de la población desempleada

[448] DAGNINO, E.: "Social recruiting: una novità da perfezionare" publicado en *Conquiste del Lavoro*, el 21 de octubre de 2014, disponible en www.bolletino adapt.it [Consulta 9/09/2015].

[449] Documento Estadísticas Osimga.org 2011, disponible en http: //www.osimga.org/export/sites/osimga/gl/documentos/d/20111201_ontsi_redes_sociais.pdf. [Consulta 05/01/2015].

[450] En algunas empresas se constituye una sección bajo el título; "Trabaja con nosotros", "Información corporativa" etc. que facilitan al demandante de empleo un formulario para introducir sus datos identificativos y profesionales. Hay otras empresas que en vez de un formulario dan una dirección de correo electrónico dónde el interesado en pertenecer a la empresa tendrá que enviar el CV asimismo, estas empresas pueden establecer un listado de vacantes en las que las personas que estén buscando un empleo podrán inscribirse una vez vistas la descripción del puesto ofertado.

[451] Internet sigue siendo el medio más escogido para captar mandos, técnicos y empleados (68,8%). Sin embargo, para la selección de directivos, se mantiene el uso de las empresas de selección (89%), Fuente: III Estudio Adecco Profesional sobre Intermediación Laboral, diciembre de 2012, disponible en http://www.adecco.es/_data/NotasPrensa/pdf/420.pdf [Consulta 12/01/2015].

que no tiene acceso a internet ni a herramientas informáticas que le ayuden a encontrar un trabajo.

2.2. Herramientas informáticas que colaboran en los procesos de búsqueda y selección de candidatos.

2.2.1. La informatización de los servicios de intermediación pública.

Actualmente el portal web del SNE[452] ofrece distintas posibilidades relacionadas con la búsqueda activa de empleo. En el portal empléate, sito dentro de la página web del SNE[453], además de fomentar servicios relacionados con la intermediación laboral se ofrecen trámites a los empresarios, Como los relacionados con la publicación de ofertas de empleo; el acceso al perfil de empresa situado en los portales de los distintos servicios de empleo autonómicos; la comunicación de contratos a estos servicios de empleo a través de la herramienta Contrat@; y comunicación de las altas, los períodos de actividad y los certificados de empresa[454]. Dentro del servicio a empresas, el SNE promueve la posibilidad de que estás se constituyan como agencias de colocación, habilitando un formulario en el que la empresa incluirá sus datos identificativos.

Es obvio que este portal sirve simplemente para dar información a las personas que quieran encontrar un empleo, por lo que se concibe como un mecanismo de información ya que la gestión de las ofertas y su vinculación con los desempleados es una competencia asumida por los SE autonómicos. A pesar de ser la intermediación laboral competencia de los SE autonómicos, curiosamente, desde la web del SEPE, se puede acceder a la web empléate, a través de la cual se le ofrecen a los demandantes de empleo una serie de servicios entre los que se encuentra su registro en el portal con la finalidad de participar en los procesos de búsqueda de empleo[455] y consultar las ofertas de empleo, aunque para esto último no es necesario el registro. Pero lo que

[452] Fuente: http://www.sistemanacionalempleo.es/informacion.html.
[453] Fuente: https://empleate.gob.es/empleo/#/.
[454] El cumplimiento de la LOPD por estos programas informáticos será analizado en el apartado 3.6 del presente Capítulo.
[455] Cuando se accede a la búsqueda de empleo, la aplicación te muestra la web www.empleate.gob, portal del empleo dependiente del Ministerio de Empleo y Seguridad Social.

permite la aplicación es que el candidato al empleo vuelva de nuevo a la página del SNE para que elija la CCAA que le interesa y pueda consultar las ofertas más destacadas en ese territorio. La web del SEPE también facilita a los demandantes de empleo información sobre las agencias de colocación que actúan en todo el territorio nacional[456].

Además, tanto en las oficinas del SEPE como en las de los SE autonómicos, se configuran lo que se conoce como "zonas TIC", que son aquéllas que intentan mejorar los servicios a la ciudadanía minimizando tiempos y simplificando trámites. Estas zonas se constituyen como espacios reservados, claramente indicados y delimitados en las oficinas de empleo, donde se ofrecen herramientas que permiten resolver, a través de medios telemáticos, los trámites laborales más frecuentes.

Cada zona cuenta con personal técnico para informar al usuario sobre las distintas opciones y posibilidades que se ponen a su alcance y guiarlo en el uso de tales herramientas. Se trata, por tanto, de intentar que el usuario adquiera la autonomía suficiente para realizar determinadas gestiones sin necesidad de personarse en las oficinas, disponiendo simplemente de una conexión a Internet y de un ordenador. Los servicios principales que ofrecen son: renovación, consulta y modificación de la demanda de empleo; impresión de documentos; informes y documentos de renovación de la demanda; consulta de ofertas de empleo; acceso a la Oficina Virtual del servicio de empleo que corresponda; acceso al portal del SEPE, etc. Para acceder a estos servicios es necesario estar en posesión de un DNI electrónico o certificado digital[457], tal y como establece el art. 13.1 de la LAECSP[458],o de un usuario y contraseña facilitado por el propio SEPE.

[456] http://www.sistemanacionalempleo.es/AgenciasColocacion_WEB/listadoAgencias.do ?Modo = inicio [Consulta 7/06/2015].

[457] La FNMT-RCM como prestador de servicios de certificación pone a su disposición diferentes tipos de certificados electrónicos mediante los cuales podrá identificarse y realizar trámites de forma segura a través de Internet. En función del destinatario de los mismos, la FNMT-RCM emite los siguientes tipos de certificados que podrá solicitar a través de nuestra SEDE Electrónica: El certificado de persona física, también denominado Certificado de usuario Clase 2 CA, es la certificación electrónica expedida por la FNMT-RCM que vincula a su Suscriptor unos Datos de verificación de Firma y confirma su identidad personal. Este certificado le permitirá identificarse de forma telemática y firmar o cifrar documentos electrónicos. El

Siguiendo la descripción de los medios tecnológicos usados en la intermediación pública, es preciso hacer mención a las oficinas virtuales de empleo. Estos servicios los ofrecen los distintos SE autonómicos y tienen como finalidad llevar a cabo tareas relacionadas con los procesos de colocación como si de una oficina física se tratase. Entre estos entes se puede señalar el sistema denominado Eureka[459], en el Servicio Andaluz de Empleo, el cual se configura como una herramienta a la que pueden acceder las empresas que tengan la necesidad de cubrir uno o más puestos de trabajo, ya que en ella están incluidos los perfiles profesionales de todas y cada una de las personas demandantes de empleo de Andalucía, tanto de aquéllas en situación de desempleo como de trabajadores en activo que pretenden mejorar sus expectativas laborales.

Una vez realizadas las búsquedas necesarias y consultados los CV de las personas candidatas, los cuales se obtienen del filtrado que realiza el propio sistema, el empresario podrá comprobar la capacitación profesional de los candidatos para decidir si pueden participar en el proceso de selección. Posteriormente, procederá al registro de la oferta para pasar después a seleccionar al conjunto de demandantes que quiere entrevistar[460]. Este sistema

---

certificado de Persona Jurídica es la certificación electrónica expedida por la FNMT-RCM que vincula a su Suscriptor (persona jurídica) unos Datos de verificación de Firma y confirma su identidad conjuntamente con la del Solicitante del certificado (persona física con poderes suficientes para custodiar dicho certificado). Este certificado es también el que deben solicitar empresas y organismos públicos para sus relaciones con la AEAT. (Fuente: https://www.cert.fnmt.es/).

[458] Art. 13.1 LAECSP: "*Las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y resulten adecuados para garantizar la identificación de los participantes y, en su caso, la autenticidad e integridad de los documentos electrónicos".*

[459] Entre las últimas aportaciones se encuentra Eureka, una aplicación informática para las empresas andaluzas que les permite gestionar ofertas de empleo por Internet en tiempo real. Eureka, el nuevo sistema de intermediación laboral por Internet puesto en marcha por la Consejería de Empleo, se enmarca en el Plan de Modernización del Servicio Andaluz de Empleo. Su lanzamiento el pasado 11 de enero de 2008, pone a disposición de las empresas andaluzas una herramienta informática que les permite realizar una intermediación laboral ágil y eficaz.

[460] En al año 2013 se produjo un aumento considerable de las ofertas difundidas telemáticamente por Eureka siendo un total de 1844 ofertas en toda Andalucía. En 2012 hay un descenso de las ofertas publicadas respecto a 2011, ya que tan sólo se publicaron 664 frente a las 790 de 2011. Este descenso también se debe a la disminución generalizada de ofertas de empleo debido a la crisis económica de nuestro país, pero lo que es cierto que estos

de intermediación laboral también es útil a la hora de gestionar los trámites relativos a las renovaciones de la demanda de empleo ya que cada vez más demandantes de empleo lo utilizan con este propósito[461]. En otras Comunidades Autónomas[462] también se incentiva la posibilidad de utilizar la oficina virtual de empleo a la hora de buscar u ofrecer un empleo, a la vez que se establece la posibilidad de renovar la tarjeta de desempleo desde cualquier ordenador o dispositivo con conexión a internet y estando en posesión, como ya se ha dicho, de un certificado digital o DNI electrónico, por lo que no es necesario acudir a las oficinas físicas de estos servicios de intermediación.

2.2.2. Instrumentos informáticos que colaboran en los procesos de búsqueda y selección de candidatos.

Las TICS, además de configurarse como mecanismos que pueden llegar a intermediar en el mercado de trabajo, también se presentan como vías de almacenamiento de datos e, incluso, herramientas colaborativas de la selección de personal. Estos instrumentos tienen repercusión tanto en la intermediación pública como privada y, evidentemente, algunos que tienen más repercusión en el ámbito privado podrán ser utilizados también en el ámbito público, sobre todo los relacionados con el registro de datos en ficheros automatizados (cloud computing).

En lo que a la intermediación pública se refiere[463], se puede decir que las tecnologías de la información, traducidas en lo que se ha denominado

---

mecanismos de difusión telemática de ofertas de empleo cada vez son más utilizados. Fuente: Sistema Observatorio ARGOS. Servicio Andaluz de Empleo.

[461] 326.982 demandantes de empleo han registrado su huella en la red de oficinas del SAE para poder acceder así a los servicios que prestan estos puntos de información y gestión, en los que se han realizado 312.994 renovaciones de demanda de empleo sin esperar colas y en un tiempo estimado de tres minutos (2008). Fuente: Estadísticas de la Consejería de Empleo de la Junta de Andalucía.

[462] Madrid: Portal de empleo de la Comunidad de Madrid http://www.madrid.org/cs/; Cataluña: Servicio de Ocupación de Cataluña http://www.oficinadetreball.cat; Comunidad Valenciana: Servicio Valenciano de Ocupación y Formación http://www.ocupacio.gva.es.; Asturias: http://www.asturias.es/site/trabajastur.

[463] Para poder entender la circulación de la información en el seno de la Administración Electrónica véase: El Documento del Trabajo sobre la Administración en línea del Grupo del art. 29 (WP 73, 10593/02/ES). En el mismo, se analizan, entre otros, las interconexiones de ficheros, el uso de la firma electrónica etc.

Administración Electrónica[464], han creado en el marco de los SEPE y de los SEP autonómicos un sistema de información para poner en relación datos de demandantes de empleo y ofertas de trabajo (SISPE)[465]. En este sentido, las TICS han supuesto grandes avances en el panorama relacionado con aquellas entidades públicas dedicadas a la gestión de las políticas activas y pasivas de empleo, pero es obvio que se han producido tratamientos de datos los cuales deben cumplir con las exigencias contempladas en la legislación que regula su protección[466], estableciéndose el respeto a la información personal como uno de los principios por los que ha de regirse el desarrollo de la Administración Electrónica[467].

Dicho sistema, regulado en la Ley de Empleo[468] y perteneciente al SNE, debe permitir al SEPE y los SPE autonómicos compartir una información básica y coordinada sobre políticas activas de empleo y prestaciones por desempleo[469]. Es un modelo mixto de gestión en el que tienen que convivir la

[464] Todo lo relacionado con las actuaciones de la Administración Electrónica está regulado en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (BOE núm. 150 de 23 de junio de 2007).

[465] El SISPE permite integrar la información relativa a la gestión de las políticas activas de empleo y las prestaciones por desempleo que llevan a cabo los Servicios Públicos de Empleo, Estatal y Autonómicos. En un modelo mixto de gestión, en el que tiene que convivir la gestión transferida a las Comunidades Autónomas (políticas activas de empleo) y la gestión estatal (prestaciones por desempleo), y que, a su vez, debe posibilitar la coordinación a nivel nacional de los planes de actuación encaminados a fomentar el empleo, el SISPE hace posible compartir, integrar y coordinar tanto la información propia de cada uno de los Servicios Públicos de Empleo, como las actuaciones y estrategias orientadas a favorecer la inserción laboral y el estudio del mercado laboral español. Fuente: nota informativa del Ministerio de Empleo y Seguridad Social, disponible en http://www.sepe.es/contenidos/inicial/sispe /pdf/NOTA_ INFORMATIVA_SISPE_310305.pdf. [Consulta 10/03/2015].

[466] Sobre este aspecto: PIÑAR MAÑAS, J.L.: "Administración Electrónica y protección de datos personales" *Dereito: Revista Xuridica da Universidade de Santiago de Compostela*, núm.1 2011, pp. 161-174; FERNÁNDEZ RODRÍGUEZ, C. Y MARTÍN MARTÍN, M.P.: "Los discursos sobre la modernización de los Servicios Públicos de Empleo: ¿hacia una nueva forma de gobernanza?". *Revista Política y Sociedad*, núm. 51, 2014, pp. 181-184.

[467] Art. 4.1 a) de la LAECSP: "*El respeto al derecho a la protección de datos de carácter personal en los términos establecidos por la Ley Orgánica 15/1999, de Protección de los Datos de Carácter Personal, en las demás leyes específicas que regulan el tratamiento de la información y en sus normas de desarrollo, así como a los derechos al honor y a la intimidad personal y familiar".*

[468] Art. 12 de la Ley de Empleo: *"El Sistema de Información de los Servicios Públicos de Empleo se configura como un sistema de información común que se organizará con una estructura informática integrada y compatible, y será el instrumento técnico que integrará la información relativa a la intermediación laboral, a la gestión de las políticas activas de empleo, y de la protección por desempleo, que realicen los servicios públicos de empleo en todo el territorio del Estado".*

[469] El programa de modernización de los SPE incluye la mejora de los recursos materiales y tecnológicos, un plan estratégico de recursos humanos y una mejora de la gestión de las

gestión transferida a las CCAA (políticas activas de empleo) y la gestión estatal (prestaciones por desempleo) y que, a su vez, debe posibilitar la coordinación a nivel nacional de los planes de actuación encaminados a fomentar el empleo.

A este efecto, en primer lugar, se establecen unas bases de datos estatales, compartida por todos los SEPE autonómicos en la que se almacenan datos comunes que pueden ser actualizados por las distintas CCAA. En segundo lugar, existen unos sistemas de información de los SE autonómicos, con bases de datos relativos a la CCAA, es decir, el SISPE facilita a la Comunidad Autónoma que pueda desagregar información de las bases de datos estatales cuando sus necesidades lo requieran. Se trata pues, de un modelo de utilización de los datos que garantiza una gestión uniforme y coordinada de los mismos en todas las CCAA[470].

Cada transacción actualiza directamente la base de datos estatal y asíncronamente, actualiza también la correspondiente base de datos autonómica. Esta modalidad es unidireccional, es decir las actualizaciones siempre se inician en el sistema estatal y terminan en diferido en el autonómico. También se puede optar por el sistema de información propio de las Comunidades Autónomas, siendo éstas las que optan por implementar y desarrollar su propio sistema de información para dar soporte a la gestión que se les transfiere[471].

Los objetivos del SISPE[472] son: promover la libre circulación y la movilidad laboral de los demandantes de empleo; favorecer la igualdad de

---

prestaciones por desempleo. Dicho programa se enmarca dentro de las directrices integradas para el crecimiento y el empleo (2005-2008) de la Estrategia de Lisboa, en concreto la directriz nº 20 que versa sobre la mejora de la respuesta a las necesidades del mercado laboral, disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:c11325 [Consulta 25/02/2015].

[470] ALUJAS RUIZ, J.A.: "El servicio público de empleo y su labor como intermediario en el mercado de trabajo en España", *Cuadernos de Ciencias Económicas y Empresariales*, núm. 53, 2007, pp. 31-34; SÁNCHEZ-RODAS NAVARRO, C.: "La orientación e intermediación directa en el empleo", *Revista Temas Laborales*, núm. 125, 2014, pp. 105-109

[471] Fuente: http://www.sepe.es/contenidos/inicial /sispe/pdf/NOTA_ INFORMATIVA_ SISPE_ 310305.pdf [Consulta 14/02/2015].

[472] El día 3 de mayo de 2005 entró en funcionamiento la aplicación SISPE, que sustituyó al antiguo sistema SILE, y que permite integrar la información de la gestión de las políticas activas de empleo y las prestaciones por desempleo, que realizan los diferentes Servicios Públicos de Empleo. Es este un modelo mixto de gestión en el que coexisten la gestión transferida a las Comunidades Autónomas (políticas activas de empleo) y la gestión estatal, permitiendo a su

oportunidades en el acceso al empleo e incrementar la capacidad de cobertura de puestos de trabajo; y compartir la información para mejorar la capacidad de intermediación. De modo que, tendrán que tener acceso a los datos de los demandantes de empleo que sean necesarios para cumplir con estas funciones[473].

Las agencias de colocación tendrán que tener, a su vez, sistemas informáticos compatibles y complementarios del SISPE[474], produciéndose de esta forma el nacimiento del Espacio Telemático Común como nexo de unión entre la agencia de colocación y el SISPE, en el cual ya se integran los datos aportados por los SEPE y distintos SEP autonómicos. A través de este mecanismo también se deberá presentar una memoria de las actividades desarrolladas por la agencia en el ejercicio anterior[475], considerando la información relativa a los indicadores de eficacia[476].

Para que las agencias puedan acceder a este sistema de transmisión de datos (ETC), tendrán que tener un usuario y clave que será proporcionada por el SEPE, siempre que previamente la agencia haya sido autorizada. Una vez

---

vez la coordinación a nivel nacional de los diferentes planes de actuación destinados a fomentar el empleo.

[473] CLIMENT RODRÍGUEZ, J. Y NAVARRO ABAL, Y.: "Oficinas virtuales de Empleo. El reto de universalizar los servicios públicos de empleo", *Revista Trabajo* núm. 24, 2011, pp. 82-83.

[474] Art. 6 del RD 1796/2010: "*La agencia de colocación tiene que disponer de sistemas informáticos compatibles y complementarios con el Sistema de Información de los Servicios Públicos de Empleo para suministrar información sobre demanda y ofertas de empleo, así como del resto de actividades realizadas como agencias de colocación".*

[475] Art. 5 n) del RD 1796/2010: "*Presentar con periodicidad anual, y dentro del primer trimestre de cada ejercicio, una Memoria de las actividades desarrolladas durante el ejercicio anterior, conteniendo, al menos, información relativa a los indicadores de eficacia contenidos en la Disposición adicional primera, así como información sobre su actividad económica como agencia de colocación".*

[476] Disposición Adicional Primera del RD 1796/2010: "*En función de lo establecido en la Disposición final tercera de la Ley 35/2010, de 17 de septiembre, los indicadores de eficacia de las agencias de colocación contemplarán, al menos, los siguientes aspectos: a. número de personas atendidas. b. número de personas atendidas perceptoras de prestaciones por desempleo. c. número de personas atendidas pertenecientes a colectivos con dificultades de inserción. d. número de ofertas y puestos de trabajo captados como resultado de su actividad de intermediación. e. número de ofertas y puestos de trabajo cubiertos con las personas atendidas como resultado de su actividad de intermediación. f. número de contratos de trabajo suscritos por las personas atendidas. g. número de contratos de trabajo indefinidos suscritos por las personas atendidas. h. otros indicadores correspondientes al resto de servicios ofrecidos por la agencia. Dichos indicadores serán evaluados cada dos años a efectos de suscripción de posibles convenios de colaboración entre las agencias y los servicios públicos de empleo".*

que la agencia de colocación introduce su código y la contraseña, proporcionados por el SEPE, puede empezar a introducir información de sus usuarios en el ETC. En un primer momento, los datos que se van a incorporar a la información integrada del SISPE son aquellos relativos al número de personas atendidas entendido en sentido amplio, pues la información del demandante de empleo no sólo se refiere al primer contacto con la agencia, sino al registro de sus datos y a la colocación, si se hubiera conseguido. También se aportan datos concernientes a colectivos con dificultades de inserción, personas con discapacidad, o aquéllos que tienen que ver con la nacionalidad del demandante de empleo[477].

Ahora bien, en el ámbito privado, se desarrollan también sistemas que permiten informatizar datos de los demandantes de empleo. Actualmente, existen algunos programas informáticos que colaboran con estas empresas de intermediación privada realizando la tarea de procesamiento y almacenamiento de datos de carácter personal. Dado que el primer paso para la selección de personal es la entrega del CV, habrá que comprobar qué vías utilizan las empresas de intermediación para realizar la tarea de clasificación de CVs[478] y el posterior almacenamiento de ese documento. Así pues, estos programas no sólo son útiles sino que también pueden resultar muy necesarios puesto que, además, ponen en práctica una serie de filtros objetivos como, por ejemplo, pasar la información curricular de aquellos candidatos que cumplan determinados requisitos profesionales, formativos, o de edad, entre otros[479]. Con el uso de estos programas informáticos de selección se clasifican a aquellos candidatos que cumplan los requisitos requeridos, reduciendo, de esta forma, los miles de CV recibidos a cientos o incluso a decenas.

---

[477] Sistema Nacional de Empleo: *Agencias de colocación. Espacio Telemático Común*, Ministerio de Empleo y Seguridad Social, 2015. pp. 3-5, 16-21, disponible en: http://www.sistemanacionalempleo.es/pdf/agencias/instrucciones_envios.pdf.

[478] LEE, I., "E-recruiting: Opportunities and challenges", *Information Management*, vol. 19, núm. 3-4, 2006, pp. 24-25; VV.AA: *Manual de selección de personal*, CEP, 2013, pp. 47-51.

[479] La empresa de selección RANDSTAD EMPLEO, utiliza el programa informático DARWIN (que es una aplicación para la validación y chequeo de datos, este programa permite hacer una criba curricular por perfiles, de todos los datos incluidos (CV) en el sistema a través de la web de la empresa (Fuente: Randstad Empleo). En MANPOWER ETT utilizan el programa de gestión de datos POWER BASE, para el registro de candidato, búsqueda de los mismos para un determinado empleo, almacenamiento de documentación relacionada con el demandante de empleo etc. (Fuente: MANPOWER ETT).

Actualmente, el mercado laboral proporciona herramientas tecnológicas que colaboran en la selección de personal, haciendo una criba de los candidatos atendiendo a su perfil psicológico, siendo quizás el más conocido el sistema experto Sigmund[480], a través del cual se intenta obtener datos cuyo tratamiento automatizado está prohibido (origen racial, nacionalidad, religión, opiniones políticas etc.) mediante unos cuestionarios exhaustivos realizados por psicólogos industriales[481]. La realización de estos test tiene como objetivo que los empresarios contraten a "trabajadores sin defectos", por lo que, cuando se realizan, son las empresas las que los califican y los trabajadores jamás conocen sus resultados. Esta clasificación de perfiles profesionales, realizada a través de este mecanismo, cataloga a los potenciales candidatos a través de criterios que no son considerados estrictamente profesionales, obteniendo un perfil más amplio que en el que se exponen características inherentes para el desarrollo de las funciones del puesto de trabajo.

Ahora bien, como consecuencia de la recopilación de gran cantidad de datos de carácter personal a través de los sistemas anteriormente descritos, se hace necesario su registro en bases de datos que, por su parte, deben respetar la privacidad. Hoy día, la utilización en algunas empresas de selección de lo que se conoce con el término anglosajón cloud computing o computación en la nube[482] para la gestión de los recursos humanos y para el almacenamiento de

[480] Sistema que permite determinar rasgos de la personalidad. El Método Sigmund es una herramienta informatizada de evaluación del Potencial, basada en competencias, consta de 436 preguntas que evalúan 37 diferentes competencias que, a su vez, responden a 10 macrocompetenciaso macrocriterios, en las Dimensiones Profesional, Social y Personal. Tras la realización de la Prueba, el Consultor mantiene una entrevista personal con el Candidato, para proporcionarle feed back explicándole los resultados obtenidos y, al mismo tiempo, ampliando aquellos datos necesarios para completar la información acerca de la candidatura. Como resultado se obtendrán un Gráfico Competencial, un Informe numérico y un Informe Individual con los comentarios del entrevistador, que se entregará al Cliente. (Fuente: Pricewaterhousecoopers)

[481] Para tratar la legitimidad de este sistema, véase lo contenido en el apartado 3.6.2. del presente Capítulo.

[482] Conjunto de dispositivos e infraestructuras de comunicaciones por los que, de manera «impredecible», pasa la información cuando se quiere transmitir de un punto a otro de Internet. Todos los elementos que se encuentran en medio de este intercambio de informaciones se han representado, tradicionalmente, como una nube. En el caso de la selección de personal y del almacenamiento de sus datos se trata de una *nube privada* en la que una entidad realiza la gestión y administración de sus servicios en la *nube* para las partes que la forman, sin que en la misma puedan participar entidades externas y manteniendo el control sobre ella.

datos es bastante generalizada. Este sistema incluye algunos software tales como; expertHRM®, que incluye módulos como la gestión de nóminas (contratación, retribución y Seguridad Social), control de presencia (asistencia y absentismo), y recursos humanos (definición del organigrama, inventario de personal, desarrollo profesional, planes de carrera y procesos de selección); el IntegRHo que es una aplicación integral de administración de recursos humanos, diseñada con las últimas tecnologías para trabajar en entorno *web*. Se puede decir que el cloud computing, además de desarrollar un sistema de almacenamiento de datos y que esos datos puedan ser consultados desde cualquier herramienta informática con conexión a internet, permite otras aplicaciones que pueden ser útiles en la selección de personal y en lo relativo a la gestión de recursos humanos en la empresa[483].

Aunque la computación en nube aporta, en cierto sentido, mayor disponibilidad y seguridad de los datos, –las empresas de cloud computing ofrecen, en su mayoría, procedimientos de backup, restore o planes de contingencia para casos de pérdidas de información o fallos que muchas empresas no tienen– esta tecnología presenta muchos riesgos relacionados con la privacidad del individuo. En general, en las empresas que contratan servicios de cloud computing existe un nivel de confianza bajo en la seguridad de los datos debido al hecho de que los datos de la empresa no están localizados dentro de la misma sino en servidores ajenos. Además, existe una cierta sensación de cautividad del cliente ya que, al no disponer de los datos en sus propias unidades de almacenamiento, se encuentra a merced del proveedor de servicios y de su proveedor de internet[484].

3. TRATAMIENTO Y CESIÓN DE DATOS EN LA SELECCIÓN DE PERSONAL.

[483] AEPD: *Guía para clientes que contraten servicios de cloud comuputing",* 2013, pp. 5-7.
[484] FERNÁNDEZ-ALLER, C.: "Algunos retos de la protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en nube (cloud computing)" *Revista de Derecho UNED*, núm. 10, 2012, pp. 132-139; OPPENHEIM, CH.: "Cloud law and contract negotiation", *El profesional de la información*, vol. 21, núm. 5, 2012, pp. 455-457.

3.1. Planteamiento general.

Una vez descritos los mecanismos de intermediación y los instrumentos que gracias a las TICS colaboran en el desarrollo de los procesos de búsqueda de empleo, es claro, de conformidad con el art. 3 a) de la LOPD, que la información que manejan estos mecanismos para el desarrollo de sus funciones se puede catalogar como de carácter personal; como es también evidente que se realizan procesamientos de datos, y prueba de ello es la inclusión de esa información de los candidatos al empleo que solicitan sus servicios en ficheros estructurados[485]. Igualmente es necesario proyectar las exigencias relacionadas con la protección de datos en relación con otro de los tratamientos que tiene lugar en la intermediación laboral como es, una vez realizada la elección del demandante de empleo más idóneo, la cesión de esos datos al empresario que lo va a contratar o a aquellas empresas externas que pueden, en un determinado momento, colaborar en las tareas relacionadas con la actividad de la empresa intermediadora.

Es cierto que la simple averiguación del dato, aunque no se someta a tratamiento, puede llegar a colisionar con el derecho a la intimidad; pero hay que tener presente que no toda lesión del derecho a la intimidad implica una afectación del derecho de a la protección de datos personales, ni viceversa, por lo que habrá que diferenciar muy claramente si los datos son efectivamente tratados o simplemente visualizados o conocidos[486]. Si bien, si se certifica finalmente la existencia de un tratamiento de datos, los instrumentos involucrados en la selección de persona ya citados tendrán que actuar en consonancia con los principios recogidos en la LOPD[487] relacionados con: la

[485] Una de las ventajas que se obtiene, con el uso de las bases de datos de los trabajadores, es la capacidad de llegar a almacenar datos que quizás de forma individual no revelen informaciones particularmente relevantes de los trabajadores pero que, si se agrupan, pueden desvelar el perfil o la personalidad de las personas que recurren a la intermediación como instrumento para encontrar un puesto de trabajo.

[486] REMOLINA ANGARITA, N.: "Aproximación constitucional de la protección de datos personales en Latinoamérica" *Revista Internacional de Protección de Datos,* vol. I, 2012, pág. 6.

[487] En España, la AEPD redactó la citada Guía de protección de datos en las relaciones laborales, 2009, disponible en: http://www.privacyconference2009.org/home/index-iden-idweb .html [Consulta 25/02/2015], destacando entre sus objetivos el de examinar aspectos de la protección de datos en los recursos humanos-selección de personal. Las recomendaciones de la AEPD en la materia se centran en aspectos muy concretos de selección de personal. Por ejemplo se recomienda disponer de modelos impresos tipos para la formalización del CV, de la

calidad o pertinencia en la petición de datos; la información que se le debe dar al titular sobre el uso y destino de su información personal; y el consentimiento para que ese tratamiento sea efectivo, impidiendo así un uso descontrolado que pueda provocar un perjuicio para el candidato al empleo[488].

Es preciso tener en cuenta, también, todas las vicisitudes que se pueden presentar en la comunicación de datos a terceros tanto en las empresas de intermediación como en todas las vías de búsqueda y almacenamiento de datos propiciadas por las TICS. Por ello, es importante resaltar todas las posibles cesiones de datos y su adaptación a lo que para ellas se establece en la LOPD.

3.2. Las distintas formas de captación de datos de los demandantes de empleo.

Una de las primeras cuestiones que se suscita está relacionada con los distintos medios que existen para captar datos de los demandantes de empleo, los cuáles se han multiplicado con la llegada de las TICs. Lo normal, cuando se pretende buscar un candidato de empleo, es publicar un anuncio de empleo en prensa, internet, buscadores de empleo, etc., donde se exponga la oferta de empleo con las características solicitadas por la empresa que persigue la

---

inserción en los anuncios o convocatorias públicas de empleo de la información contenida en el art. 5 de la LOPD, el establecimiento de pautas de acuse de recibo en la entrega del CV por parte del candidato, etc. Sin embargo, estas recomendaciones no dejan de ser reiterativas de lo estipulado en la LOPD, a diferencia de lo que ocurre en la CNIL que, con la instauración de la *Guidepour les employeurs et les salaries* 2010, disponible en: www.cnil.fr/file admin/documents/Guides_pra tiques/Guide_employeurs_salaries.pdf., se hace un estudio del dato concreto que se necesita para proceder a realizar una correcta selección de personal. En la guía francesa se puede encontrar, incluso, la mala práctica generada en lo que concierne a los comentarios vertidos por el departamento de selección de personal. Además se tratan dos aspectos claves: por un lado, el derecho que tiene el candidato a disponer de los análisis y evaluaciones de su candidatura y, por otro, la recomendación de obtener el consentimiento del candidato cuando se vaya a enviar su CV a empresas que mantengan oculta su identidad. También, al igual que hace la AEPD, la CNIL recoge tratamientos específicos para los datos sensibles, aunque en la CNIL se presenta una lista más detallada. Sobre este aspecto, vid. TOLEDO BAÑEZ, C.: "La protección de los datos personales y las relaciones laborales en España y Francia: Análisis de las recomendaciones dela AEPD y la CNIL como ejercicio de derecho comparado previo a una traducción jurídica", *Revista Crítica de Historia de las Relaciones Laborales y de la Política Social*, núm. 1 y 2, 2010, pp. 49-52.

[488] DE VICENTE PACHÉS, F.: "Protección de datos personales y agentes intermediarios de colocación; la tutela de la libertad informática-intimidad del demandante de empleo", *Revista del Consejo Económico y Social (CES),* núm. 64, 2012, pp. 5-7.

contratación de un trabajador[489], y es a partir de este momento cuando la agencia de intermediación, o la propia empresa que demanda el trabajo, empiezan a recibir información de los potenciales candidatos. Esta información puede llegar a través del envío del currículo por correo ordinario o por vía telemática, aunque el candidato también puede inscribirse en la oferta a través del formulario habilitado en la propia web de la empresa que necesita cubrir ese empleo o de la agencia de intermediación correspondiente, formulario en el que deberá introducir sus datos personales y profesionales.

En este primer momento, el candidato aporta información relevante como puede ser la referida a datos identificativos, formación, puestos desempeñados anteriormente, edad, etc. No obstante, el candidato al empleo, como conoce que esta primera información es de suma importancia para intentar captar la atención, suele incluir muchos datos no sólo de carácter personal sino también los que considera que resaltan mejor sus cualidades para ajustar su CV lo máximo posible al puesto y al tipo de empresa al que se dirige.

Otra de las formas de captar datos de los candidatos de empleo es la realización de una serie de pruebas de selección, siendo las más habituales las de conocimientos, ejercicios prácticos, profesionales, psicotécnicos, dinámicas de grupo, etc. Por ejemplo, es frecuente la utilización de baterías de test como una de las pruebas iniciales que el candidato debe afrontar para seguir en el proceso de selección. Además de estas pruebas, lo habitual es que el candidato se someta a una entrevista de trabajo en la que el entrevistador u

[489] El empresario debe ser especialmente cuidadoso a la hora de configurar los perfiles que solicita, pues en ocasiones puede pedir otros datos no profesionales, los cuales están estrechamente vinculados con sus circunstancias familiares. Es evidente, que el candidato en principio no tendría que hacer ninguna declaración sobre estas informaciones, pues no son relevantes para valorar su aptitud como candidato a una oferta de trabajo determinada. Estas situaciones podría generar una clara discriminación en el acceso al empleo, si, por ejemplo, realizan una oferta de empleo alegando la contratación sólo de hombres que no tuvieran cargas familiares. Sobre este aspecto vid.: SÁNCHEZ-URÁN AZAÑA, Y.: "Garantía jurisdiccional del derecho a la no discriminación en la relación de trabajo", *Revista del Ministerio de Trabajo y Asuntos Sociales*, núm. extraordinario sobre igualdad efectiva de mujeres y hombres, 2007, pág. 190.; CORDERO GORDILLO, V.: *Igualdad y no discriminación de las personas con discapacidad en el mercado de trabajo,* Tirant lo Blanch, 2011, pág. 100; MOLINA NAVARRETE, C.: "Derecho con mirada de mujer: la solución al conflicto de conciliación de la vida laboral y familiar en la STC 3/2007, de 15 de febrero", *Diario La Ley*, año XXVIII, núm. 6681, 2007, pág. 23.

oferente de empleo realiza una serie de preguntas acerca de las condiciones personales y profesionales de los candidatos. Como es lógico, en esta última fase de la selección de trabajadores es dónde se recoge más información ya que con las preguntas realizadas en la entrevista se amplían y precisan los datos contenidos en el CV. Igualmente se pueden aplicar técnicas de evaluación grupales, las cuales se proponen observar, explorar, reconocer, comparar y conocer aspectos referidos a los candidatos al empleo tales como características personales, habilidades, recursos y posibilidades en relación con otras personas interactuando con ellas. Con estas técnicas grupales se pretende evaluar cómo resuelve, cómo afronta, cómo compite, cómo expresa sus ideas el candidato, valorando también el resultado de este análisis comparado con el puesto de trabajo que se oferta[490].

Todas las formas anteriormente descritas de captación permiten un acceso a los datos de carácter personal, al margen de si son incluidos o no en un fichero. Sin embargo, con la repercusión que las TICS han tenido en la gestión de personal, sobretodo en cuanto a la recogida, normalmente de forma electrónica, de los datos contenidos en los CV, parece difícil pensar que los sujetos que requieren información de los demandantes de empleo tan sólo se dediquen a visualizar los datos, entre otras cosas porque el mero hecho de recibirlos a través de estos medios informáticos favorece de forma natural su almacenamiento en las bases de datos de la empresa.

Además, la información que se puede obtener, por ejemplo, de las redes sociales[491] y los buscadores de empleo es mayor que la que obtendría si se utilizara el método tradicional de recepción física de CVs. La búsqueda de candidatos a través de las redes sociales, pues, permite averiguar información

[490] Sobre las técnicas de selección: HERNÁNDEZ LAHOZ, M. Y GIL LACRUZ, M.: "Proceso y técnicas de selección" *Revista Capital Humano*, Año nº 24, Nº Extra 257, 2011, pp. 36-43; VV.AA.: *Manual de selección de personal,* Ed. CEP, 2011, pp. 83-91; OLLERO IZARD, M.: *El proceso de captación y selección de personal,* Gestión, 2000, pp. 80-82; VV.AA.: *Guía Técnica y de Buenas Prácticas en Reclutamiento y Selección de Personal*, Colegio Oficial de Psicólogos de Madrid, 2009, pp. 22-33.

[491] III Estudio Adecco Profesional de diciembre de 2012: "Se duplica el uso de las redes sociales para reclutar candidatos: el 48,7% de las empresas ya las emplea". Las empresas de intermediación son conscientes que cada vez más personas en su tiempo libre se relaciona a través de las redes sociales y deciden acercarse a ellas por medio de este canal para ofrecerle cualquier oportunidad laboral".

sobre los mismos cuyo uso inadecuado es una amenaza a la esfera íntima del demandante de empleo. Además, este acceso a los datos de los candidatos, realizada a través de la red social, lo puede practicar cualquier empleador con la mera creación de una cuenta en la misma y, de esta forma, hacer la selección de personal sin necesidad de contratar los servicios de una agencia de intermediación[492].

3.3. Aplicación de los principios de la LOPD al tratamiento de datos realizado por la intermediación laboral.

Como ha previsto la LOPD, es preciso respetar una serie de principios cuando se realiza el tratamiento de datos de carácter personal, el primero de los cuales es el de calidad de los datos. Con este principio se pretende limitar, precisamente, la libertad del intermediador para almacenar datos sobre aspectos que nada tengan que ver con la posible incorporación de ese candidato a la empresa; debiéndose comprobar que la utilización de esos datos es adecuada o tiene relación con la finalidad que propició su recogida, prohibiéndose, por tanto, el acopio de información que no sea necesaria para la correcta selección del candidato. Pues bien, de conformidad con estos criterios, el agente de intermediación tan sólo podrá recopilar información que le permita certificar la capacidad profesional de ese candidato para el puesto de trabajo ofertado[493]; lo que no excluye que pueda suponer, en ocasiones, la inclusión de determinados rasgos de la personalidad si estos se consideran necesarios para realizar la prestación de trabajo y siempre que su averiguación sea proporcional y no excesiva[494].

---

[492] Sobre el incremento de reclutamiento mediante Web 2.0, como imposición sobre anteriores modelos también virtuales, véase; GIRARD, A. Y FALLERY, B.: "E-recruitment: new practices, new issues. An exploratory study", en *Proceedings of the Third International Workshop on Human Resource Information Systems*, INSTICC Press, Milan, 2009, pp. 39-48; ROJAS, P.: *Reclutamiento y selección 2.0: la nueva forma de encontrar talento,* Editorial UOC, 2010, pp. 9-17; ORTIZ LÓPEZ, P.: "Redes Sociales: funcionamiento y tratamiento de información personal", en VV.AA.: *Derecho y Redes Sociales,* Aranzadi, 2013, pág. 24.

[493] Sobre este aspecto véase lo establecido en el art. 4.1 de la Recomendación CM/Rec del Comité de Ministros de la UE sobre el tratamiento de datos personales en el contexto del empleo de 1 de abril de 2015: *"Los empleadores deberían minimizar el tratamiento de datos personales sólo a los datos necesarios para la finalidad perseguida en los casos de que se trate".*

[494] DEL REY GUANTER, S.: "Tratamiento automatizado de…", op. cit., pág. 20.

Hay que tener en cuenta, como se ha repetido ya, que la aplicación de las técnicas de selección en los procesos de intermediación tiene que tener como objetivo proporcionar un empleo a la persona desempleada así como a la empresa un candidato idóneo para el puesto de trabajo que demanda, siempre que su uso garantice la salvaguarda de la información personal de los demandantes de empleo. Lo que se pretende, entonces, es lograr un equilibrio entre la necesidad que tiene el empresario de conocer al candidato y el derecho de éste de preservar sus datos de carácter personal[495]. Obviamente, y debido a la propia función de los procesos selectivos, debe evitarse obtener y procesar información irrelevante para el desarrollo de la actividad[496], como sucede con datos, por ejemplo, acerca del estado civil de la persona ya que esta información es innecesaria para comprobar la capacidad profesional del candidato al empleo, pudiendo, en un determinado momento, suponer una discriminación en el acceso al empleo si se tiene en cuenta la situación personal del trabajador para descartarlo del proceso de selección[497].

---

495 MING TING-DING, J Y DÉNIZ DÉNIZ, M.C.: "La selección del personal como un proceso ético y eficiente: el caso de la entrevista personal" en AYALA CALVO, J.C.(coord.).: *Conocimiento, innovación y emprendedores : camino al futuro*, Universidad de la Rioja, 2007, pp. 3559-3562.

496 En sede jurisprudencial se avala la recogida de datos relativos a la intimidad del trabajador si estos son necesarios para un buen desempeño de la actividad laboral, véase; la Sentencia del TSJ de Justicia de Castilla y León de 3 de diciembre de 1996 (AS 1996, 3998): "...consideró justificadas las preguntas sobre la vida privada y personal de los trabajadores contenidas en un test al que la empresa RENFE sometía al personal de circulación (conductores de puentes grúas, carros trasbordadores, carretillas) para evitar accidentes y reducir el índice de peligrosidad en el manejo de maquinaria pesada. Establecería en relación a los test psicológicos que ahondan en aspectos íntimos de la personalidad del trabajador (sociabilidad, inteligencia), tres *requisitos que deben reunir las pruebas para respetar el derecho a la intimidad del trabajador: el candidato debe prestar su conformidad a someterse al test, el candidato debe conocer el tipo de test que va tener que desarrollar y cuáles son los objetivos que se persiguen con ello; el psicólogo que corrige el test sólo puede informar al empresario de los datos objetivos del candidato que sean necesarios para el desarrollo del puesto de trabajo al que se aspira. Ahora bien, en relación a la primera cuestión (conformidad), el pronunciamiento del tribunal adolece de irreal al manifestar que aun cuando algunas preguntas inciden en la esfera privada y familiar de los trabajadores, su contestación es facultativa o voluntaria y no necesaria «es, en definitiva, el titular del derecho quien delimita y protege su intimidad personal, sin que la mera sugerencia o indicación de la empresa de colaboración o actitud positiva y no meramente omisiva, pueda considerarse como agresión del derecho personal, al no incorporar la negativa consecuencia perjudicial para el encuestado".*

497 En este sentido vid., Sentencia del TSJ de Canarias de 7 de abril de 2014(AS 2014\2179): "*Así las cosas, ha quedado acreditado en autos que el día 26 de mayo de 2009, en el curso de una entrevista de trabajo que la empresa "AENA AEROPUERTOS, SA" celebró en sus instalaciones del Aeropuerto Tenerife Norte para nuevas contrataciones de Titulados, los entrevistadores (Dª Reyes y D. Melchor) preguntaron a la aspirante Dª Lorenza , casada y madre de dos niñas menores, que se desplazó desde Valladolid a Tenerife para participar en el proceso de selección, por su situación personal (marido, hijos) y le hicieron presente las dificultades que tendría para encontrar colegio para sus hijas y para que su marido consiguiera trabajo en la Isla y le advirtieron que no querían a alguien que se cogiera una baja por*

En todo caso, quedarían fuera del concepto de averiguación prohibida, aquellos hechos o datos que resulten de general conocimiento o incluso que tengan una difusión pública; por ejemplo, cuando el intermediador laboral conoce que el demandante de empleo tiene una determinada ideología política, debido a las múltiples apariciones en campañas políticas, incluso en radio y televisión, que haya hecho ese candidato[498]. En estos supuestos, el intermediador podrá estar al tanto de esa información al igual que cualquier ciudadano como consecuencia de las manifestaciones públicas que el trabajador ha realizado y que pueden determinar sus afinidades políticas, por lo que en este supuesto no existiría un incumplimiento del principio de calidad[499].

En cuanto a la forma de obtención de los datos, y todavía dentro del principio de calidad, es necesario considerar el caso de la obtención de los mismos por la empresa de intermediación haciendo uso de medios ilícitos. En este punto cabe señalar que el agente intermediador no podrá recoger información a través de mecanismos o procedimientos prohibidos o mediante sujetos extraños a la relación existente entre éste y el demandante de empleo. A modo de ejemplo, se puede hacer referencia a las escuchas telefónicas, las

---

maternidad, teniendo que confesar Dª Lorenza que se había ligado las trompas y que no podía tener más hijos. Concluida las entrevistas, fue seleccionada para cubrir el puesto la otra candidata finalista que concurría con la actora, Dª Cecilia, que a las mismas preguntas respondió que no tenía pareja ni hijos".

[498] Análogamente y como ejemplo de la posibilidad de tratar datos referidos a aspectos que no tengan que ver con las cualidades profesionales del candidato, véase el supuesto en el que la averiguación de la ideología de un representante sindical se realiza como consecuencia de la notoriedad pública del mismo. En este sentido destaca la Sentencia de la Audiencia Nacional de 12 de junio de 2014 (JUR 2014\193394), la cual puede aportar constancia y justificación a lo expuesto en el texto aunque no se trate de una caso acaecido en agencias de intermediación laboral: *Por otro lado, hay que tener en cuenta que el denunciante ostenta un cargo público, como es ser Secretario General de un Sindicato, y dicho cargo unido a su nombre era conocido públicamente a través de los medios de comunicación. Hay que tener en cuenta que el papel desempeñado por el denunciante en la vida pública, puede hacer que la injerencia en sus derechos fundamentales se encuentre justificada por el interés preponderante de dicho público en tener acceso a la información de que se trate (Sentencia del Tribunal de la Unión Europea de 13 de mayo de 2014 (TJCE 2014, 85) -Asunto C-131/12 -). En consecuencia, la Sala estima que el sindicato recurrente ha obrado en legítimo ejercicio de su derecho a la libertad sindical en la vertiente de su derecho a informar sobre hechos relevantes y de interés para los trabajadores, y de sus libertades de expresión e información en relación con aquel, facilitando información de interés público acerca de la actividad sindical, que en la ponderación con el derecho a la protección de datos personales del denunciante que en el presente caso nos concierne debe prevalecer sobre este.*

[499] GOÑI SEÍN, J.L.: *El respeto a la esfera privada del trabajador. Un estudio sobre los límites del poder de control empresarial*, Civitas, 1988, pp. 50-52.

grabaciones, las manifestaciones hechas por carta etc., o cualquier otra fórmula que oculte el verdadero fin de la recogida de información[500]. Siendo posible que estas actuaciones puedan constituir, incluso, una conducta castigada por la normativa penal, además de suponer un trato discriminatorio en el acceso al empleo y un atentado al derecho a la intimidad, si es el caso que se llegan a averiguar características o conductas personales que son irrelevantes para el desempeño de la actividad que se va a realizar en la empresa.

Siguiendo con el principio de calidad de los datos, constituye una exigencia ineludible el especial cuidado en cuanto a la información que se persigue en el desarrollo de la entrevista de selección, de los test psicológicos y de las pruebas de selección. Las entrevistas de selección se presentan desde una doble perspectiva, ya que, por un lado, pueden servir para completar e incluso realzar el CV; pero, por otro lado, también pueden ser aprovechadas para recoger más información de la realmente necesaria para la selección del trabajador. No obstante, el intermediador incurrirá en mala fe si es consciente de la inexistente relación entre esa información y la valoración del perfil profesional del candidato por lo que, en este caso, se estaría sin duda

[500] Sobre la recogida de datos a través de medios fraudulentos, vid., Sentencia de la Audiencia Nacional de 22 de septiembre de 2011 (RJCA 2011\730); "*También insiste la parte recurrente en que los datos aportados eran ciertos (nombre, domicilio, números de cuenta, números de teléfono, etc.) por lo que resulta que no consta acreditado que haya existido fraude alguno en la recogida de datos; también entiende que el contrato se formalizaba entre UNI2 y los particulares por lo que es la mercantil contratante la que asume el riesgo de la contratación y la que formaliza el contrato y presta el servicio y se hace responsable de la veracidad de los datos.La infracción imputada a Comercial Redes Sistelcom SA es la prevista en el artículo 4.7 LOPD (RCL 1999, 3058) , según el cual: " Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos" , siendo el artículo 44.4.a) de la misma Ley Orgánica el que considera como infracción muy grave " La recogida de datos de forma engañosa o fraudulenta". Preceptos de los que deriva la necesidad de que los datos personales que se recojan en cualquier fichero sean obtenidos por medios lícitos, y de esta forma sea conocida su utilización por los afectados, siendo los responsables de su obtención quienes responden del cumplimiento de esta obligación. Procederá aplicar, para dar solución a la cuestión que se plantea, el criterio que dimana de la sentencia dictada por esta Sala en el recurso 149/2006 (JUR 2008, 11666) dictada en relación a la misma empresa ahora recurrente aunque la solución final, por las circunstancias de cada caso, no pueda ser la misma. Aplicando este precepto al caso objeto del presente recurso resulta que Comercial Redes Sistelcom no ha negado, ni por ende desvirtuado, que en los contratos de preasignación aparezcan firmas que no se corresponden con las de las personas que se determinan como suscriptores de dichos contratos, ni tampoco que no coincida el número de DNI de uno de los supuestos clientes, y a pesar de ello, los datos personales de los repetidos denunciantes fueron dados de alta por Sistelcom en la página web de Jazztel".*

vulnerando el principio de calidad de datos. Respecto de los test psicológicos[501], éstos tendrán que ser delimitados, es decir, deben ser consecuentes con la finalidad para la cual se realizan que no es otra que la consecución de un empleo. Por este motivo, estos test tampoco deben llegar a desvelar datos íntimos del trabajador que nada tengan que ver con el buen desempeño de su actividad laboral[502] ya que, si así fuera, irían en contra de lo establecido en el principio de calidad pues el objetivo de su recogida y posterior tratamiento no estaría relacionado con lo previsto en el momento de la petición de la información[503].

La obligación de cancelar los datos a instancia, en este caso, de la empresa de intermediación también viene contemplada dentro del principio de calidad[504], atendiendo al derecho que tiene el titular del dato a que sus datos sean cancelados cuando haya finalizado el objetivo que propició la recogida de sus datos personales por la agencia de intermediación. En cuanto al alcance del derecho de cancelación, hay que diferenciar dos situaciones: la de los candidatos al empleo que han sido rechazados en el proceso de selección; y la de aquéllos que por el contrario han sido admitidos y que van a ser contratados para prestar servicios en la empresa. Por tanto, es necesario ilustrar en qué momento un dato de carácter personal deja de ser necesario para la finalidad

[501] Con la realización de test psicológicos, se pueden averiguar datos relacionados con la salud mental del trabajador los cuales tendrán que ser tratados de forma especial con las exigencias contenidas en el art. 7 y ss. de la LOPD. Quizás dónde se establecen pautas más rígidas para el tratamiento de estos datos sea en lo relativo a la forma de prestar el consentimiento, puesto que, el titular del dato tendrá que dar su consentimiento expreso y por escrito para que se produzca el mismo (art. 7.2 LOPD).

[502] DATTNER, B.: "El uso y el mal uso de los test de personalidad", *Revista Capital Humano*, núm.182 (Especial selección de personal), 2004, pp. 24-28; VV.AA**.:** *Los test de selección de personal: inteligencia–personalidad*, Deusto, 2003, pp. 31-36**;** VV.AA.: "Datos perdidos y propiedades psicométricas en los test de personalidad*", Anales de psicología*, núm. 29/1, 2013, pp. 285-292.

[503] Si se incumpliera con alguno de los principios, entre los que se encuentra el principio de calidad, la LOPD prevé las sanciones descritas en los arts. 44 y ss. de la LOPD.

[504] Art. 4.5 de la LOPD: *"Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados".*

que fundamentó su obtención, no siendo posible establecer un límite temporal genérico[505].

En el primer caso, es lógico que la finalidad por la que se recogieron esos datos haya terminado, sobre todo si una empresa de intermediación solicita, a través de los medios que dispone, CVs para un puesto de trabajo concreto. Una vez otorgado éste a alguno de los candidatos, el resto de CVs ya no son necesarios, pues su finalidad era la de formar parte de ese determinado proceso de selección, por lo que tendrán que ser destruidos de forma confidencial[506], es decir, como consecuencia de la cantidad de información personal existente en los CVs, es preciso contratar los servicios de una empresa dedicada a esta actividad y sometidas a la confidencialidad debida para que estos datos no sean revelados y se destruyan, sin que puedan volver a tratarse[507]. Si bien podría justificarse el no ejercicio de la cancelación de los datos por la empresa de intermediación si el titular de los datos permitiera que sus datos permanecieran en los ficheros de la empresa para poder participar en futuros procesos de selección[508]. En el segundo caso, el derecho a la cancelación de los datos no existe prácticamente, o al menos no de forma total, ya que siempre se podría defender su mantenimiento como condición para una mejor y más eficiente gestión del personal, incluso si se trata, como sería lo deseable, de datos que han podido ser sólo relevantes en el proceso de selección[509].

---

[505] DONOVAN, C.: "Data protection and the retention of personal data: how long is too long?" Computer Law and Security Report, vol. 20, Issue 6, 2004, pp. 434 y ss.

[506] Las pautas para proceder a la destrucción de forma confidencial de documentos vienen establecidas en la Norma UNE 15713:2010 (Comité Europeo de Normalización), la cual establece el código de buenas prácticas que deberían cumplir las empresas dedicadas a la destrucción confidencial de documentos.

[507] La destrucción de datos de forma confidencial dependerá del soporte en el que se encuentre esta información. Evidentemente, si los datos se encuentran en papel la forma más habitual de destruirlos será a través de una máquina destructora de papel. No obstante en España existen empresas dedicadas a este cometido como, por ejemplo, Deletedoc, D+S, Reduce y también algunos programas de borrado de software muy útiles para aquellos datos automatizados, como pueden ser: Disk Wipe, Freeraser, DISKExtinguishero.

[508] Consultas realizadas a ETTS y agencias de colocación, para ver qué política emplean cuando los datos dejan de ser necesarios puesto que la finalidad para la que fueron recabados ha concluido. ETTs consultadas Randstad Empleo, Addecco y Grupo Crit. En la mayoría se guardan los CV para futuros procesos de selección, justificando este hecho en el beneficio que conlleva para el desempleado el estar al corriente de otras ofertas y que se pueda contar con él para futuros procesos de selección.

[509] También la Recomendación CM/Rec del Comité de Ministros de la UE sobre el tratamiento de datos personales en el contexto del empleo de 1 de abril de 2015 hace referencia a los

En otro orden y para dar cumplimiento al principio de información en el tratamiento de datos, los mecanismos de intermediación establecen lo que se conoce como políticas de privacidad, las cuales incluyen pautas sobre qué destino y uso de le va a dar a la información de los usuarios que acuden a los servicios de intermediación. Con la inclusión de estos datos en las condiciones de uso o políticas de privacidad de la empresa parece solventarse la obligación de informar a los titulares de los datos sobre lo establecido en el citado art. 5 de la LOPD[510].

Esta información sobre el tratamiento de datos también puede darse por medio de los impresos normalizados o informatizados en la web que los demandantes de empleo cumplimentan con el objetivo de que puedan insertarse en los distintos itinerarios de selección. Ahora bien, actualmente no es frecuente completar formularios en soporte papel, siendo lo habitual la recepción de información curricular a través de email o por medio de un formulario habilitado en su página web con ese objetivo.

Así pues, una vez preseleccionado el candidato y citado para la entrevista de trabajo pertinente, el candidato al empleo que asiste a una entrevista de trabajo debe conocer que podrá negarse a contestar aquellas cuestiones que entienda que no tienen relevancia para valorar su aptitud profesional. Esta negativa del desempleado depende mucho de las

---

distintos supuestos en los que se va a proceder a conservar los datos de carácter personal obtenidos en los procesos de búsqueda de empleo, vid., art. 13.2: *"Los datos personales presentados en apoyo de una solicitud de empleo normalmente deberían suprimirse tan pronto como se hace evidente que una oferta de empleo no se hará o no es aceptada por el solicitante de empleo. Cuando estos datos se almacenan con miras a una oportunidad de trabajo adicional, el interesado debe ser informado en consecuencia y los datos debe suprimirse si él o ella se lo pide".*

[510] Art. 5 de la LOPD: "*Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento".*

explicaciones que le haya proporcionado el propio intermediador; de forma que éste deberá manifestar que tales informaciones son imprescindibles para poder certificar la capacidad profesional teniendo en cuenta la naturaleza de la oferta de trabajo.

Además de lo previsto en el art. 5 de la LOPD, sobre la información que se le debe dar al titular del dato relativa a su tratamiento, se debe informar a los demandantes de empleo de la creación de un fichero de datos común para varias sucursales, sobre todo en aquellas empresas de intermediación que tienen filiales en otras ciudades o, incluso, fuera de España, y que están coordinadas para las tareas de selección, por lo que podrán utilizar los datos para fines relacionados con la colocación del futuro trabajador. Con este hecho lo que se pretende es informar al demandante de empleo y titular de los datos acerca de las distintas empresas que van a tratar esa información, pudiéndose considerar, incluso, este hecho una comunicación de datos a terceros[511] ya que la empresa que recoge esos datos los archiva en un fichero común que puede ser consultado por otras empresas del grupo, información que tendrá que conocer ese candidato al empleo.

Aunque la normativa sobre protección de datos establece detalladamente los extremos sobre los que hay que informar a los candidatos a un empleo, esta obligación de informar sobre el tratamiento de datos se puede eximir cuando la misma se deduzca de las circunstancias en que se recaban los datos o de su propia naturaleza. Esta advertencia normativa, trasladada a la selección de personal, significa que esta información se puede obviar cuando el candidato conoce la forma de actuación de la empresa de intermediación, pues se sobreentiende que ese tratamiento lo que pretende es facilitarle su búsqueda de empleo[512].

[511] La cesión o comunicación de datos a terceros va a ser analizada en el apartado 3.5 del presente Capítulo.
[512] MESANZA LEGARDA, S.: "*Efectos de la protección de datos de carácter personal en la gestión de recursos humanos"* Congreso Internacional de Gestión de RRHH en Administración Pública, 2007, pp. 16-19.

En tercer lugar, las agencias de intermediación tendrán que cumplir con el principio del consentimiento, ya que se precisa el asentimiento del titular del dato para cualquier tratamiento de su información personal que pretenda realizarse; si bien en este aspecto existe una laguna legal en lo relativo a los procesamientos de datos realizados en el ámbito de la intermediación laboral pues el art. 6.2 de la LOPD establece que ese consentimiento podrá exceptuarse cuando esos datos tengan que tratarse para el mantenimiento de una relación precontractual. Por tanto, en este punto y teniendo en cuenta las labores de la agencias de intermediación mediante la realización de tareas conducentes y previas a la contratación del candidato al empleo, se podría excluir al intermediador de la obligación de requerir el consentimiento al interesado al considerar que esas actividades pueden ser calificadas como de naturaleza precontractual. Aparte de que ese consentimiento está implícito, a posteriori, en la perfección del contrato de trabajo pues se materializa con su realización.

Ahora bien, puede ocurrir que, por los motivos que sean, finalmente no se llegue a contratar al trabajador, dejando en estos casos desprotegidos los datos de ese trabajador que se han podido llegar a tratar sin su consentimiento[513]. Por este motivo, un tratamiento preliminar tendría que realizarse con la conformidad del titular del dato, teniendo en cuenta que esos actos de selección de personal generan incertidumbre en lo referente a la

[513] Sentencia del TSJ de Madrid de 30 de junio de 2008 (AS 2008\2186); " *Es cierto que el art. 6.1 de la LO 15/1999, de 13 de diciembre de Protección de Datos, establece que el tratamiento de datos de carácter personal requerirá el consentimiento inequívoco del afectado. Pero, y a continuación, y como excepción a la regla general, igualmente establece "salvo que la Ley disponga otra cosa", para añadir, acto seguido y en su núm. 2, que "no será preciso el consentimiento cuando los datos de carácter personal... se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento", ….Esto es lo acaecido en el caso de autos, pues en definitiva se trata del desarrollo de una campaña de soporte de telemarketing, consistente en prestar asistencia telefónica a los clientes de la empresa principal, y para ello es necesario la aportación por la contratista de unos mínimos datos personales del trabajador adscrito a tales cometidos, a fin de poder entrar en contacto con las bases de datos de sus clientes, lo que se revela así en indispensable, tanto para el mantenimiento de dicha vinculación, como para el cumplimiento del contrato de trabajo, por lo que ha de concluirse que en tal supuesto no es necesario el previo consentimiento del trabajador afectado, siendo por tal razón irrelevante que dicho consentimiento expreso conste prestado después de iniciada la relación mercantil entablada entre ambas patronales, que es, en esencia, el único argumento del recurso de la Comunidad de Madrid".*

contratación del trabajador[514]. No obstante, si finalmente opera esta excepción al consentimiento, deberá en todo caso rodearse de ciertas garantías que puedan evitar un tratamiento de datos que pueda perjudicar al demandante de empleo. Estas garantías tienen relación con el hecho de que, aunque el consentimiento no tenga que prestarse para cada caso concreto, la empresa de intermediación deberá de informar en la recogida y del tratamiento de datos que se pretende realizar, lo que tiene como finalidad preservar aquellas informaciones de los candidatos que finalmente no son contratados y que, evidentemente, no prestan su consentimiento ni previamente ni materializado en la contratación laboral[515].

En cuarto y último lugar es preciso hacer referencia a las medidas de seguridad que se tienen que implantar cuando esos datos quedan registrados en los ficheros de las empresas de intermediación[516]. Lógicamente, si estas agencias de intermediación almacenan la información captada de los demandantes de empleo, deben cumplir con lo establecido en la LOPD sobre la seguridad de los datos y la confidencialidad en su tratamiento[517]. Para ello, se configuran las distintas medidas de seguridad –nivel básico, medio y alto – atendiendo a la naturaleza de los datos guardados. A su vez, estos ficheros deberán estar recogidos en un fichero, automatizado o no, y el responsable del fichero estará obligado a notificar la creación del fichero[518] ante la AEPD a través del formulario habilitado por ésta en su página web.

---

[514] VV.AA.: *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova. 2012, pág. 106; TASCÓN LÓPEZ, R.: "Principios de la protección de datos: consentimiento del afectado. Los ficheros empresariales sobre trabajadores y los derechos de los mismos en el marco de la relación contractual con el empleador" *Estudios y comentarios legislativos Civitas,* 2010, pp.112-115*;* FERNÁNDEZ VILLAZÓN, L.A.: "Tratamiento automatizado de datos personales en los procesos de selección de trabajadores", *Revista Relaciones Laborales,* núm. 1, 1994, pág. 28, 531; DE VICENTE PACHÉS, F.: *El derecho del trabajador al…,* op. cit.*,* pp. 143-153; DE VICENTE PACHÉS, F; "Protección de datos personales y agentes*…",* op. cit., pág. 10; VALVERDE ASENCIO, A.: "El derecho a la protección…", op. cit., pp. 366-370.

[515] TASCÓN LÓPEZ, R.:"La protección de datos personales…", op. cit., pp. 485-494; TRONCOSO REIGADO, A.: *La protección de datos…,* op. cit., pp. 1563-1567.

[516] Esta obligación es inherente al responsable del fichero y según lo establecido en el art. 3 d) de la LOPD las empresas de intermediación ostentan esta categoría desde el mismo momento en que almacenan datos en sus ficheros.

[517] Vid. Arts. 9 y 10 de la LOPD.

[518] Art. 26.1 y 2 de la LOPD; *"1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos. 2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del*

Obviamente, de entre todas las entidades de intermediación analizadas la que quizás realiza un tratamiento de datos más amplio como consecuencia de su facultad de contratar al demandante para cederlo a la empresa usuaria, sea la ETT, que tendrá que constituir distintos tipos de ficheros con datos de carácter personal[519]; por ejemplo, si se han realizado reconocimientos médicos antes de entrar en la empresa, ésta tendrá un fichero con datos de salud de los trabajadores[520]; en otro fichero constarán los datos económicos de los trabajadores para el pago de las nóminas; otro con los datos profesionales; y así sucesivamente.

En este sentido, hay que hacer alusión a la Resolución 00371/2009 de 4 de marzo de 2009 de la AEPD[521], en la que se sanciona a una empresa de trabajo temporal por abandonar documentos en la calle. Estos documentos no estaban almacenados en ningún fichero estructurado -estaban recogidos en cajas de cartón-, y se tendría que haber tomado en consideración una serie de medidas de seguridad debido a que lo contenido en estas cajas son datos de carácter personal de candidatos a ofertas de empleo. A este respecto, la AEPD ha establecido que: "*ha quedado acreditado que la ETT no adoptó las medidas de índole técnica y organizativas necesarias que garantizasen la seguridad de los datos de carácter personal de sus trabajadores, de manera que se evitase, en este caso, el acceso no autorizado" quedando también acreditado que la ETT, responsable de la custodia de los datos en cuestión, se vulneró el deber de secreto garantizado en el artículo 10 de la LOPD, al haber*

---

fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros".

519 Estos ficheros son de titularidad privada ya que tienen como responsables a las personas, empresas o entidades sometidas al derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que son responsables las corporaciones de derecho público, mientras dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

520 Estos datos son considerados datos especialmente protegidos, tal y como se menciona en el art. 7.3 de la LOPD; *"Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente".*

521 Disponible en http://www.agpd.es/portalwebAGPD/resoluciones/ procedimientos_ sanciona dores / ps_2009 /common/pdfs/PS-00481-2008_Resolucion-de-fecha-04-03-2009_Art-ii-culo-9-LOPD.pdf. [Consulta 07/01/2015].

posibilitado el acceso no restringido a datos personales básicos de sus trabajadores, sin consentimiento de sus titulares[522]*".*

Es posible que los datos tratados en la intermediación laboral se guarden en ficheros sitos en distintos ordenadore o en una base de datos común que pudiera consultarse desde cualquier soporte informático; y también, si estos ficheros no estuvieran informatizados, podrían estar duplicados dentro de la misma oficina o en distintas sedes de la agencia. No existe solución clara sobre este asunto, ya que ni la LOPD ni la Directiva 95/46/CE han dicho nada de forma explícita, por lo que no existe la obligación de que el fichero tenga que estar ubicado en un único sitio y, en este sentido, ha contestado la AEPD en su informe 368/2003[523]. También las personas que presten servicios a la empresa fuera del centro de trabajo tendrán que velar por la seguridad de la información personal que traten y, por tanto, estos intermediarios necesitan una autorización previa del responsable del fichero para que de esta forma se pueda garantizar el nivel de seguridad correspondiente[524].

---

[522] Sobre la infracción del establecimiento de medidas de seguridad, la AEPD, se basa en las Sentencias de la Audiencia Nacional, Sala de lo Contencioso- Administrativo, Sección Primera, Recursos 1182/2001, de fecha 7 de febrero de 2003 (2006\275713), 1517/2001 de 15 de octubre de 2003 (JUR 2004\53521), 160/2006 de 3 de octubre de 2007 (JUR 2007\316013). La primera de ellas, en el Fundamento de Derecho Tercero señala: "*No basta, entonces, con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto. Y, por supuesto, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Así, de nada sirve que se aprueben unas instrucciones detalladas sobre el modo de proceder para la recogida y destrucción de documentos que contengan datos personales si luego no se exige a los empleados del banco la observancia de aquellas instrucciones (...) se trataba de documentos de uso interno a los que no debían tener acceso personas ajenas al organigrama de...y si lo tuvieron fue de manera anómala, esto es, por una insuficiencia o deficiente puesta en práctica de las medidas de seguridad".*

[523] Según la AEPD: " *En consecuencia, de lo establecido en la Directiva y en la propia Ley Orgánica parece desprenderse que el concepto de fichero no va directamente vinculado a la exigencia de que el mismo se encuentre en una única ubicación, sino que será posible la existencia de ficheros distribuidos en lugares geográficos remotos entre sí, siempre y cuando la organización y sistematización de los datos responda a una conjunto organizado y uniformado de datos, sometido a algún tipo de gestión centralizada".* Informe jurídico 368/2003 de la AEPD, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/inscripcion_ficheros/common/pdfs/2003-0368_Inscripci-oo-n-de-ficheros-situados-en-m-uu-ltiples-ubicaciones.pdf. [Consulta 9/06/2015].

[524] Art. 86 del RDLOPD: "*Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas".*

3.4. Problemas derivados del tratamiento de datos del conocido como sistema de selección 2.0.

Delimitado[525] lo que se entiende por selección 2.0, el tratamiento de datos a través de estos medios carece de una normativa específica, por lo que habrá que acudir a lo establecido en la LOPD y en el RDLOPD, sin olvidar lo que sobre la misma cuestión establece la LSSI y la Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información[526]. Sobre este asunto la AEPD también ha dictado alguna que otra resolución, al igual que el Grupo del art. 29 que ha emitido varios dictámenes, como se verá más adelante. También desde Europa se han dado algunas Recomendaciones sobre lo que se conoce como tratamiento de datos en internet, las cuáles serán analizadas en el apartado relativo a los buscadores webs de empleo[527].

Lógicamente, no todas las consultas de los perfiles que se hacen en las redes sociales o de lo inserto en los buscadores de empleo constituyen un tratamiento de datos, ya que puede ocurrir que los intermediadores laborales accedan al perfil de un candidato simplemente para consultarlo, sin que este hecho constituya un tratamiento de datos de los definidos en el art. 3. c) LOPD. Ahora bien, la recopilación o grabación de esos datos o la cesión de los mismos a terceros, sí constituye un tratamiento de datos de carácter personal respecto del cual es necesario que se cumplan los principios de la LOPD.

Lógicamente la selección 2.0 es un instrumento al alcance de cualquier ciudadano, pero en este apartado se va a analizar el tratamiento de datos que realiza la empresa de intermediación y el propio empresario a la hora de buscar posibles candidatos de empleo. Por ello, es necesario analizar, por un lado, si estas redes sociales cumplen con el principio de información plasmado en su política de privacidad para que en un momento posterior los usuarios de la red social consientan el tratamiento de sus datos allí contenidos y, por otro, certificar que los sujetos que están en situación de búsqueda de trabajadores respeten los principios de la LOPD a la hora de captar y almacenar información

[525] Véase apartado 2.1 del presente Capítulo.
[526] BOE núm. 312 de 29 de diciembre de 2007.
[527] Vid. apartado 3.4.2 del presente Capítulo.

de esos usuarios de la red social o buscadores de empleo[528], debido a la amplia gama de servicios que ofrecen como intermediadores de empleo.

En términos generales la política de privacidad establecida en las webs de los mecanismos de selección 2.0 y en otros instrumentos informáticos que colaboren con la selección de personal pretende informar a los titulares de los datos que se insertan en esos portales de internet acerca de su utilización, teniendo en cuenta lo dispuesto en el art. 5 de la LOPD. Además, hay que indicar que cualquier página web debe implantar lo que se conoce como aviso legal que es un texto en el que se debe contener los datos identificativos del titular de la web[529].

La política de privacidad, suele colocarse al pie de la página web, no obstante, legalmente, únicamente es necesario que se coloque en una zona accesible y visible para el usuario. Ahora bien, además de lo anterior, en caso de que la web disponga de un formulario de contacto donde el usuario introduce sus datos personales (nombre, correo electrónico, etc.) es necesario que, previamente a que el usuario envíe sus datos personales a través del sitio

[528] ESTEVE PARDO, A.: "Uso de datos personales por parte de google y facebook y protección de la intimidad en Europa Y Estados Unidos" en VV.AA.: *Internet, Derecho y Política. Regulating Smart Citie*. Actas del XI Congreso Internacional, Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona 2-3 Julio, 2015. Barcelona: UOC-Huygens Editorial, pp.154-163

[529] Art. 10 de la LSSI: *" Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información: a) Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva. b) Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.c) En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión. d) Si ejerce una profesión regulada deberá indicar: 1.º Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.2.º El título académico oficial o profesional con el que cuente. 3.º El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento. 4.º Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos. e) El número de identificación fiscal que le corresponda. f) Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío".*

web, acepte la política de privacidad de la página web. Para ello, normalmente, se utiliza un "checklist" en el que se pone un texto tipo a "*he leído y acepto la política de privacidad de este sitio web*" (con enlace al texto legal completo). El usuario deberá marcar el checklist para poder enviar sus datos personales a través de la web.

Obviamente el incumplimiento por parte del prestador de servicios webs de todo lo relacionado con la implantación de la política de privacidad tiene una doble repercusión. Por un lado, se trata de una infracción grave del art. 44.3 de la LOPD y, por otra parte, si se trata de la ausencia de esta información en un servicio web[530] la LSSI también prevé esta actuación como una infracción con su correspondiente sanción[531].

3.4.1. Pautas de privacidad en el tratamiento de datos en las redes sociales.

En la Resolución sobre protección de la privacidad en los servicios de redes sociales, aprobada en la 30ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad[532], lo que se pretendía era advertir a los usuarios de redes sociales que fueran consecuentes con la información que publicaban, teniendo en cuenta la facilidad de acceso que tenían los terceros para visualizar el perfil completo de una persona; pues, en la mayoría de las ocasiones, es muy complicado eliminar la información sobre ellos. Esta facilidad se traduce en el simple hecho de poner el nombre completo de una persona en el buscador Google, indagando este buscador información relativa,

[530] Art. 22.2 de la LSSI: "*Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre , de protección de datos de carácter personal. Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones. Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario".*

[531] Vid., art. 38.4 g) y 39.1 c)

[532] Estrasburgo, 15-17 de octubre de 2008, disponible en https://www.agpd.es/portalwebAGPD/canaldcumentacion/conferencias/index-ides-idphp.php#inter. [Consulta 22/05/2015].

entre otras, a si esa persona tiene una cuenta en una red social y pudiendo, entonces, acceder al perfil completo sin necesidad de introducir ninguna clave ni ningún otro requisito de acceso[533].

En España, la sentencia del Tribunal Supremo de 15 de octubre de 2015[534] es la primera resolución acerca de lo que se conoce como derecho al olvido digital. En ella se establece que las informaciones perjudiciales que afecten a personas sin relevancia pública no deberán estar accesibles en los buscadores de internet cuando el paso del tiempo haya hecho perder relevancia a la noticia. La decisión del Pleno de la Sala Civil establece que en esos supuestos los propios medios de comunicación deberán encargarse de impedir que la noticia pueda ser archivada en los buscadores de internet. La resolución está directamente vinculada con la dictada el año pasado por el Tribunal de Justicia de la UE en el llamado 'caso Google'.

Por tanto, esta sentencia puede suponer un punto de inflexión para eliminar datos de estos buscadores masivos, ya que "*va perdiendo su*

[533] En reciente jurisprudencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 (Caso Google Spain contra AEPD) (TJCE\2014\85); "*A este respecto, debe señalarse, en primer lugar, que, como se ha afirmado en los apartados 36 a 38 de la presente sentencia, un tratamiento de datos personales como el controvertido en el litigio principal, efectuado por el gestor de un motor de búsqueda, puede afectar significativamente a los derechos fundamentales de respeto de la vida privada y de protección de datos personales cuando la búsqueda realizada sirviéndose de ese motor de búsqueda se lleva a cabo a partir del nombre de una persona física, toda vez que dicho tratamiento permite a cualquier internauta obtener mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet , que afecta potencialmente a una multitud de aspectos de su vida privada, que, sin dicho motor, no se habrían interconectado o sólo podrían haberlo sido muy difícilmente y que le permite de este modo establecer un perfil más o menos detallado de la persona de que se trate. Además, el efecto de la injerencia en dichos derechos del interesado se multiplica debido al importante papel que desempeñan Internet y los motores de búsqueda en la sociedad moderna, que confieren a la información contenida en tal lista de resultados carácter ubicuo".* Véase en el mismo sentido Sentencia del TJUE (TJCE 2011, 331) y Sentencia de la Audiencia Nacional de 29 de diciembre de 2014 (RJCA 2015\181). Sin embargo, la reciente Sentencia del Tribunal Supremo de 14 de marzo de 2016 (rec.1380/2015, disponible en www.cendoj, ROJ: STS 964/2016) establece que el responsable del tratamiento ante el que se tendrá que efectuar cualquier reclamación relacionada con la eliminación de datos en el motor de búsqueda Google no será Google Spain, sino Google inc.: *"…la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, finalmente, ponerla a disposición de los internautas, debe calificarse de "tratamiento de datos personales", en el sentido de dicho artículo 2, letra b), cuando esa información contiene datos personales; y, por otra parte, el gestor de un motor de búsqueda, que en este caso y de manera incontrovertida es Google Inc., debe considerarse "responsable" de dicho tratamiento, en el sentido del mencionado artículo 2, letra d), en tanto que determina los fines y medios de esa actividad de motor de búsqueda".*

[534] Disponible en www.cendoj.es , ROJ (STS 4132/2015).

justificación a medida que transcurre el tiempo si las personas concernidas carecen de relevancia pública y los hechos, vinculados a esas personas, carecen de interés histórico, pues aunque el tratamiento de los datos pueda considerarse veraz, ya no resulta adecuado para la finalidad con la que inicialmente fueron recogidos y tratados y distorsiona gravemente la percepción que los demás ciudadanos tienen de la persona afectada, provocando un efecto estigmatizador e impidiendo su plena inserción en la sociedad". Por lo que, su mantenimiento vulneraría el principio de calidad de los datos al considerar que el hecho de mantener indexada la información, cuando ya había perdido toda relevancia posible, no cumple con la adecuación, pertinencia, proporcionalidad y exactitud exigida para el tratamiento de los datos de carácter personal.

Frente a lo anterior, los proveedores de servicios de redes sociales profesionales pueden justificar el cumplimiento del principio de información, sosteniendo que en la política de privacidad establecida en sus redes sociales se advierte a los usuarios de todas las actuaciones que se van a efectuar respecto al tratamiento de sus datos de carácter personal. A través de esa política de privacidad se informa, también, sobre la posibilidad de los usuarios de restringir el acceso a su información implantando distintos niveles de privacidad según su propio criterio. Es evidente que la mayor parte de los usuarios de redes sociales no suelen consultar esas pautas de privacidad, por lo que quizás esas reglas debieran estar más a su alcance o ser más visibles. Así pues, se puede decir que existe poca transparencia a la hora de informar sobre las posibilidades de acceso que van a tener los terceros a los datos de carácter personal de quienes acceden a dichas redes sociales.

En este sentido no se está cumpliendo con una de las recomendaciones dadas en la citada 30ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad relativas, por un lado, a la poca visualización o difícil acceso que normalmente se tiene a la información sobre la privacidad y, por otro, a los riesgos de seguridad acentuados por los probables accesos que pudieran darse por parte de terceros. También, establece que estos

proveedores tendrán que controlar la utilización que los interesados hacen de la comunidad, restringiendo la visibilidad completa de los perfiles si el usuario no ha establecido los parámetros de privacidad pertinentes, para evitar que su perfil aparezca de forma completa y perceptible para cualquier persona.

Partiendo, pues, de la base de que las reglas de privacidad están contenidas en sus políticas se puede observar cómo lo primero que se menciona es que con las mismas lo que se persigue es justamente mantener la privacidad de los datos de los usuarios. De manera que tan sólo podrán acceder y tratar los datos aquellas personas que pertenezcan a su lista de contactos; siendo esto así, las empresas de intermediación sólo podrán acceder al perfil del candidato al empleo que previamente lo haya aceptado para formar parte de su lista de contactos. En cualquier caso, se puede decir que existen redes sociales de ámbito profesional que no cumplen con esta exigencia protectora de la privacidad; así sucede con la red social profesional LinkedIn donde se permite en un primer momento y a cualquier usuario acceder al perfil de otros sin que sea necesario pertenecer a su red de contactos; de forma que la restricción del acceso a los datos de los usuarios tan sólo operaría si esta posibilidad se hubiera contemplado previamente a la configuración de su perfil.

En ocasiones, el consentimiento que se presta, aceptando la política de privacidad, para tratar esa información no engloba cualquier tipo de tratamiento, sino sólo aquél encaminado a la obtención de un empleo, pues esa será la finalidad principal de la red social profesional[535]. Por esta razón, en la configuración de las redes sociales se suele pedir el consentimiento del titular del dato a la hora de crear una cuenta en la red, informándole, además, acerca de que los datos contenidos en el perfil podrán ser vistos por otros si media el consentimiento de su titular[536]. A pesar de solicitar el consentimiento del

[535] Dictamen 15/2011 sobre la definición del consentimiento del grupo de Trabajo del art. 29, adoptado el 13 de julio de 2011, pp. 20-22.
[536] Política de privacidad red social LinkedIn, disponible en https://es.linkedin.com/; *"Al facilitarnos información personal cuando creas o actualizas tu cuenta y tu perfil, estás aceptando expresa y voluntariamente los términos y condiciones de las Condiciones de uso de LinkedIn, y aceptas y consientes libremente en que procesemos tu información personal en los modos establecidos en esta Política de privacidad. El suministro de información por tu parte,*

interesado para procesar su información personal, existen determinados datos que siguen estando restringidos, como los relacionados con la inclusión de los usuarios en grupos de opinión y los relativos a la dirección de correo electrónico, siendo necesario en este caso volver a pedir el consentimiento del titular para tratar estos datos.

Un ejemplo de política de privacidad lo constituye la red social Xing donde se indica, entre otros aspectos, que la protección de los datos de carácter personal recogidos se hará de conforme a lo establecido en la normativa alemana sobre protección de datos, señalando también que Xing utilizará la información allí contenida, pero no podrá cederla ni comunicarla a terceros ni siquiera con fines publicitarios, comerciales o con cualquier otro propósito sin que medie el consentimiento del titular de los datos. Así pues, el interesado será el único que podrá decidir sobre qué datos de carácter personal pueden ser vistos o cedidos a otros usuarios de la red social. Cada vez que el usuario añade un dato a la red social, ésta le interroga sobre la posibilidad de que estos datos sean visibles para terceros, lo que indica el grado de respeto que se otorga en esta red social al principio del consentimiento. Finalmente, para establecer contacto con algún usuario de Xing, se tendrá que enviar un mensaje privado a través de la plataforma al contacto con que se quiera mantener alguna relación profesional, y sólo se podrá ver su perfil completo si éste acepta la invitación[537].

Por otra parte, además de informar en la política de privacidad de los tratamientos de datos que se van a efectuar, es necesario que los sujetos que buscan candidatos a través de las redes sociales atiendan a lo contemplado en la LOPD, si realmente llegan a procesar la información que obtienen de esta herramienta informática. En primer lugar, a través de las redes sociales es posible realizar entrevistas profesionales, por ejemplo, mediante videoconferencia, sin que sea necesario que el solicitante de empleo, al que previamente se ha preseleccionado, se traslade a la sede de la agencia de

incluida cualquier información considerada "delicada" por la legislación aplicable, es un acto enteramente voluntario".

[537] Política de privacidad de la red social profesional XING, disponible en https:// www.xing.com/privacy [Consulta 02/02/2015].

intermediación para ser entrevistado por los consultores. El problema que se puede plantear con realización de una entrevista con estas características es el relacionado con el destino que van a tener los datos recogidos. Lo lógico sería que estas informaciones tan sólo sirvieran para valorar al candidato, pero con esta acción se posibilita tanto el archivo de su imagen como de las respuestas dadas a las preguntas realizadas por el entrevistador, configurándose esta grabación como un tratamiento de datos que, como tal, debe respetar los principios de la LOPD[538].

En consecuencia, esa información deberá usarse con la única finalidad de evaluar la aptitud del candidato al empleo, sin tener en cuenta otros aspectos que se puedan derivar de su grabación que el intermediador tiene oportunidad de visualizar en distintos momentos posteriores a la realización de la entrevista. También se tendrá que informar al demandante de empleo sobre qué personas van a visualizar esos datos y sobre las posibles cesiones a terceros que pudieran darse, siempre con la finalidad de contribuir a facilitar la búsqueda de un empleo. En consecuencia, no sólo es importante informar al candidato en el momento de registrarse en la red social, sino que también es preciso hacerlo cada vez que se vaya a realizar una gestión que implique un tratamiento de datos de carácter personal. Además se debe advertir también de la inclusión de los datos en un fichero así como de los datos de la persona que va a ostentar la condición de responsable del mismo.

En estos supuestos, la prestación expresa del consentimiento se puede excepcionar[539] puesto que se considera que puede ir implícita si finalmente se contrata al trabajador, demostrando así que el tratamiento de datos tiene como único objeto que el demandante de empleo consiga un trabajo. Sin embargo, en este punto cabría hacer una matización, teniendo en cuenta que a la entrevista de trabajo acude más de un candidato y que la excepción al consentimiento sólo operaria para el candidato o candidatos que finalmente

[538] BARRIUSO RUIZ, C.: "Las redes sociales y la protección de datos hoy" *Anuario de la Facultad de Derecho*, núm. 2, 2009, pp. 320-327; CAMPUZANO TOMÉ, H.: "Marco regulador de la protección de datos de carácter personal en las redes sociales digitales" *Actualidad Civil*, núm. 6, 2011, pp. 3-6.
[539] Véase art. 6.2 de la LOPD.

firmen el contrato de trabajo por lo que, como ya se ha concluido, tiene sentido la petición del consentimiento en la recogida del dato para tratarlo, independientemente de la expectativa que exista de contratación laboral.

En segundo lugar, es evidente la utilidad que tienen las indagaciones de información de los candidatos que se hagan por medio de las redes sociales, sobre todo si se accede a redes sociales no profesionales, pues se pueden conocer otros datos de los demandantes de empleo que van más allá de los meramente profesionales para, finalmente, proceder a su selección o no. Sin embargo, lo lógico es que, si lo que se pretende es valorar todo lo relacionado con el perfil profesional del candidato, estos intermediarios laborales acudan sólo a lo establecido en las redes sociales profesionales, no examinando otros aspectos de la vida personal del candidato al empleo ya que estas redes no permiten que se puedan colgar fotos y comentarios que nada tengan que ver con la consecución de un empleo[540].

Es cierto que, para justificar estas acciones, se puede sostener que el acceso y posterior tratamiento de las distintas informaciones del candidato al empleo puede enriquecer mucho el proceso de selección, pero lo que no puede es configurarse como un medio que llegue a condicionar la decisión de seleccionar al trabajador, salvo que estas averiguaciones pudieran afectar de forma notoria a la normal ejecución de la prestación de servicios que se le ofrece[541]. Sólo en estos casos podría tener sentido tratar esa información o tenerla en cuenta para el proceso de selección porque realmente podría formar parte de la certificación de la capacidad profesional del candidato al empleo.

Para los sujetos que utilicen las redes sociales como herramienta en los procesos de búsqueda de trabajadores, estas actuaciones se pueden

[540] DÍAZ LLAIRÓ, A*.: El talento está en la red*, Lid Editorial, 2011, pp. 190-192; GAMERO, R.: "Servicios basados en redes sociales, la Web 2.0", *Boletín de la Sociedad de la Información: Tecnología e Innovación*, vol. 6, núm. 9, 2006, pp. 5-8; AEPD: *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online.* 2008, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/ com mon/Estudios/estudio_inteco_aped_120209_redes_sociales.pdf. [Consulta 13/06/2015].
[541] CARDONA RUBERT, M.B.: "La utilización de las redes sociales en el ámbito de la empresa" *Revista de Derecho Social*, núm. 52, 2010, pág. 72.

configurar como pruebas selectivas con la ventaja, para la empresa, de que los candidatos no saben que están siendo evaluados, por lo que no se está cumpliendo lo previsto en la LOPD referido al principio de información que debe estar presente en el tratamiento de datos. En consecuencia, se debería informar al candidato de que se va a buscar en las redes sociales datos sobre su comportamiento y, también, de los posibles usos y procesamientos que se vayan a realizar con esa información captada por medio de la red social.

Por este motivo y para poder salvaguardar lo que se conoce como reputación "online", el titular de los datos y usuario de la red social deberá conocer las opiniones insertadas en la red social por otros contactos de su red cuyos comentarios pueden ser visualizados por terceras personas con acceso a su perfil, sobre todo para prevenir que el agente de intermediación pueda conocer aspectos personales de los distintos candidatos y tenerlos en cuenta para decidirse por una futura contratación[542]. Con esto se quiere decir que, el sistema –red social- no aporta las garantías suficientes para proteger los datos de forma debida ya que podría haber restringido el acceso desde un primer momento dejando al usuario la facultad de permitir el acceso cuando lo estimara oportuno y no al revés, como ocurre en la actualidad. Es obvio que el problema radica en la falta de observancia tanto de las políticas de privacidad contenidas en la red social como de los parámetros a seguir para restringir el acceso a la información personal contenida en este medio.

En este mismo sentido argumenta el Gobierno español[543] ante la consulta planteada sobre la necesidad de promover un marco legal que proteja a las personal contra las opiniones vertidas en las redes sociales. La respuesta a esta consulta[544] gira en torno a la voluntariedad de las redes sociales, en el

[542] LLORENS ESPADA, J.: "El uso de facebook en los procesos de selección de personal y la protección de los derechos de los candidatos" *Revista de Derecho Social*, núm.68, 2014, pp. 53-66; CALVO GALLEGO, J.: "TIC y poder de control empresarial: reglas internas de utilización y otras cuestiones relativas al uso de Facebook y redes sociales" *Revista Doctrinal Aranzadi Social,* núm. 9, 2012, pp. 16-18.
[543] BOCG 184/090219 núm. D-456 de 8/10/2010 pág. 73 y BOCG núm. D-508 de 14/01/2011 pág. 107.
[544] Art. 34.1 de la Ley de Empleo: *"La intermediación laboral realizada por los servicios públicos de empleo y las agencias de colocación, así como las acciones de intermediación que puedan realizar otras entidades colaboradoras de aquéllos, se prestarán de acuerdo a los principios*

sentido de que el usuario es el que puede elegir si las quiere utilizar y el que tiene potestad para establecer el método de protección de sus datos de carácter personal, afirmando que la búsqueda de información de carácter personal que puede realizar el intermediador laboral sobre un determinado candidato a través de este medio es la misma que pudiera realizar cualquier otra persona.

Esta respuesta no aporta nada nuevo, puesto que ya se sabe que cualquier persona puede entrar en el perfil de otra, pero habrá que tener en cuenta que existen disparidades en lo relativo a las finalidades que tienen determinados sujetos y está claro que el intermediador laboral lo que pretende es completar la información de un posible candidato a un empleo. En este sentido, existe indefensión para los demandantes de empleo, ya que es realmente sencillo el registro del intermediador en una concreta red social, en la medida en que se puede inscribir como particular con la intención de averiguar datos de carácter personal de los demandantes y utilizarlos para su selección de personal con otras finalidades[545].

---

constitucionales de igualdad de oportunidades en el acceso al empleo y no discriminación, garantizándose la plena transparencia en el funcionamiento de los mismos. Los servicios públicos de empleo, agencias y entidades señalados en el párrafo anterior someterán su actuación en el tratamiento de datos de los trabajadores a la normativa aplicable en materia de protección de datos". Incluso, se califica como infracción muy grave en el art. 16.2 del Real Decreto Legislativo 5/2000 de 4 de agosto por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones del Orden Social (BOE núm. 189 de 8 de agosto de 2000): *"Solicitar datos de carácter personal en los procesos de selección o establecer condiciones, mediante la publicidad, difusión o por cualquier otro medio, que constituyan discriminaciones para el acceso al empleo por motivos de sexo, origen, incluido el racial o étnico, edad, estado civil, discapacidad, religión o convicciones, opinión política, orientación sexual, afiliación sindical, condición social y lengua dentro del Estado".*

[545] En nuestro país, la creación de un perfil falso de un tercero en una red social está sancionado por la AEPD con una multa de 2.000 € al infringir lo dispuesto en el artículo 6.1.de la LOPD sin perjuicio de otras responsabilidades en otras jurisdicciones, vid., Resolución AEPD R/01716/2011 de 27 de julio de 2011, Procedimiento núm. PS/00137/2011, disponible en http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2011/common/pdfs/PS-00137-2011_Resolucion-de-fecha-27-07-2011_Art-ii-culo-6.1-LOPD.PDF. [Consulta 06/05/2015]. En Alemania se aconsejó prohibir el uso de Facebook por el empleador para buscar candidatos para una oferta de empleo, (Proyecto de Ley Federal 25 de agosto de 2010), intentando limitar con esta medida el rastreo virtual de los perfiles de Facebook u otras redes sociales no profesionales que permiten al empleador, o encargado de la selección de personal de una empresa, acceder a más datos de los realmente necesarios para realizar una correcta política de selección de personal. De forma que las empresas podrán seguir buscando en Internet informaciones acerca de los aspirantes, pero solo allí donde está permitido, es decir, en redes profesionales como LinkedIn, en las que las personan publican informaciones relativas a sus experiencias de trabajo.

Aunque estos hechos pudieran no tener importancia ya que el personal de selección podrá concertar una entrevista personal en la cual solicite al entrevistado los documentos necesarios para averiguar si los datos insertos en la red social son ciertos o no, la averiguación de más datos, no pertinentes para valorar la capacidad del trabajador, puede hacer que algunos candidatos sean rechazados desde un primer momento y no tengan siquiera la oportunidad de acudir a la entrevista de trabajo. Por lo que, además de incumplir con el principio de calidad de los datos por el tratamiento de datos excesivos o no pertinentes para el fin acordado, este hecho pudiera ser constitutivo de una discriminación en el acceso al empleo, pues habrá candidatos que tan sólo serán valorados por lo ocurrido en la entrevista y, en cambio, los que sí tienen perfil en la red pueden ser descartados antes de acudir a ella , encontrándose, por este hecho, en desigualdad de condiciones en el acceso al proceso de selección.

En esta misma materia, es interesante remitirse al Dictamen 5/2009 del Grupo del art. 29 sobre las redes sociales en línea, adoptado el 12 de junio de 2009[546]. Su objetivo principal es proporcionar orientaciones a los proveedores de SRS en cuanto a las medidas que deben establecerse para garantizar el cumplimiento de lo establecido en la Directiva 95/46/CE, estableciéndose la exigencia a los prestadores de servicios de un reforzamiento del derecho del usuario a la protección de datos de carácter personal, resaltando, como forma de garantizar la privacidad, la obligación de informar sobre el destino de los datos y la identidad de la empresa que presta el servicio.

[546] Este documento está disponible en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf [Consulta 14/06/2015]. Existen otros trabajos y documentos sobre el tema, utilizados para la redacción del Dictamen, como es el caso del Memorándum de Roma, disponible en: http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491, adoptado en marzo de 2008 por el Grupo de Trabajo internacional de Berlín sobre protección de datos en las telecomunicaciones [Consulta 26/12/2014]. Este Memorándum analiza los riesgos que para la intimidad y la seguridad presentan las redes sociales y proporciona directrices a los reguladores, proveedores y usuarios. O la Resolución sobre la protección de la vida privada en los servicios de redes sociales, adoptada en la 30 Conferencia internacional de los Comisarios responsables de la protección de datos y la vida privada en Estrasburgo, donde se analizan los retos que plantean los servicios de redes sociales. Por último, el Grupo 29 tiene en cuenta también el documento de orientación publicado en octubre de 2007 por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), titulado *Cuestiones de seguridad y recomendaciones para las redes sociales en línea*.

El Dictamen 5/2009 considera primordial la preservación del ámbito privado para que se pueda impulsar el uso de las redes sociales como mecanismo que fomente la conexión entre candidatos al empleo con aquellas entidades que lo ofrecen[547], deteniéndose en algunas consideraciones. En primer lugar, que las empresas de intermediación laboral son, en principio, simples usuarias de la red sin que sobre ellas recaiga responsabilidad alguna en el tratamiento de datos de carácter personal que pudieran hacer. No obstante, puesto que la finalidad del uso de la red social no es otra que la búsqueda de candidatos para las ofertas de empleo que ellas gestionan, no deben considerarse, por tanto, exentas de responsabilidad, que se imputa sólo a los proveedores de la red social[548], teniendo que asumir las obligaciones inherentes a un responsable del tratamiento si de la utilización de las redes sociales captaran informaciones de los candidatos que fueran finalmente archivadas en un fichero en sus dependencias.

En segundo lugar, el Dictamen también hace mención, en su apartado 3.8, a las pautas a seguir en cuanto a la conservación de los datos contenidos en la red social[549]. La fijación de estas pautas sobre la conservación de los

[547] VELA SÁNCHEZ-MERLO, C; "La privacidad de los datos en las redes sociales", *Revista Española de Protección de Datos,* núm. 5, 2008, pp. 246-249; CARDONA RUBERT, M.B.: "Redes sociales y contrato de trabajo" en VV.AA.: *Derecho y redes sociales*, Civitas, 2010, pp. 169-170 y 176.

[548] En este sentido, y siguiendo lo que establece el apartado 3.1.1 del Dictamen 5/2009 la empresa de intermediación podría ser responsable del tratamiento de datos ya que; "*Si un usuario de SRS actúa en nombre de una empresa o de una asociación o utiliza el SRS principalmente como una plataforma con fines comerciales, políticos o sociales, la exención no se aplica. En este caso, el usuario asume la plena responsabilidad de un responsable del tratamiento de datos que revela datos personales a otro responsable del tratamiento de datos (SRS) y a terceros (otros usuarios de SRS o incluso, potencialmente, a otros responsables del tratamiento de datos que tienen acceso a ellos)".*En estos casos será necesario el consentimiento del titular del dato para poder ceder esa información a terceros.

[549] Apartado 3.8 Dictamen 5/2009; "*Algunos SRS (Abreviatura) conservan también los datos de identificación de los usuarios suspendidos del servicio, con el fin de garantizar que ya no podrán registrarse de nuevo. En tal caso, estos usuarios deben ser informados de que se está realizando tal tratamiento. Además, la única información que puede conservarse es la información de identificación y no las razones por las que se suspendió a estas personas. Esta información no deberá conservarse durante más de un año. Los datos personales comunicados por un usuario cuando se registra en un SRS deberían suprimirse en cuanto el usuario o el proveedor de SRS decida suprimir la cuenta. Del mismo modo, la información suprimida por el usuario cuando actualice su cuenta no debería conservarse. Los SRS deberían informar a los usuarios antes de proceder a estos trámites, a través de los medios de que disponen, sobre estos períodos de conservación. Por razones jurídicas y de seguridad, en algunos casos específicos, podría justificarse conservar datos y cuentas actualizados o suprimidos durante un*

datos viene a solucionar la ausencia de regulación sobre este tema de la LOPD ya que en ella tan sólo se hace alusión a la cancelación de datos y a su posible conservación para algunos casos[550].

Otra cuestión es la relativa a la posibilidad de conservar los datos cuando los usuarios han sido suspendidos o cuando han dejado de usar la red social. En este sentido, el Dictamen considera adecuado que los datos, pero únicamente los identificativos, se almacenen durante no más de un año y con la única finalidad de que no vuelvan a registrase en la red social, lo que no tiene mucho sentido pues un usuario, en un determinado momento, puede decidir no formar parte de la red social, por las circunstancias que sean, pero en un futuro se le debería permitir volver a configurar su cuenta en la misma si así lo decide. En el supuesto de que el mantenimiento de los datos en la red sea consecuencia de una falta de uso, el Dictamen se decanta por la obligación de informar a los usuarios de la desactivación de la cuenta.

Otro de los problemas que se pueden presentar, en lo que se refiere a la protección de los datos de carácter personal, es el relacionado con la ubicación de estas redes sociales ya que muchas de ellas no están en territorio español y no se rigen por la normativa española. En este sentido, habrá que atender a la legislación del país dónde tenga su sede la red social, surgiendo problemas si en el país en cuestión no existe legislación que proteja los datos de los usuarios de las redes sociales; una cuestión que se trata en el apartado dedicado a la protección de datos en las transferencias internacionales de ellos[551].

3.4.2. Buscadores webs de empleo y protección de datos.

período de tiempo determinado con el fin de contribuir a impedir las operaciones maliciosas resultantes de la usurpación de identidad y demás infracciones o delitos. Cuando un usuario no utiliza el servicio durante un período determinado, el perfil debería desactivarse, es decir, dejar de ser visible por otros usuarios o por el mundo exterior y, después de otro periodo, los datos de la cuenta abandonada deberían suprimirse. Los SRS deberían informar a los usuarios antes de proceder a estos trámites a través de los medios de que dispongan".

[550] Vid., art.16 de la LOPD.

[551] Vid. pág. 101 y ss. del presente capítulo.

Ante la falta de regulación específica que trate las posibilidades del tratamiento de datos en los buscadores webs de empleo, hay que recurrir a las reglas generales establecidas en la LOPD. Sin embargo, existe algún documento que contempla el tratamiento de datos de carácter personal en internet, como por ejemplo puede ser la Recomendación del Comité de Ministros del Consejo de Europa sobre la protección de la vida privada en internet[552] en la que se insertan una serie de principios que se aconseja, aunque no de forma vinculante, que sean observados tanto por los usuarios como los proveedores de servicios de Internet. Por otra parte, el Grupo del art. 29 también ha realizado una gran labor para intentar adecuar los principios de la protección de datos al uso que se hace de ellos en internet, elaborando dos Recomendaciones en las que, por un lado, se establecen pautas sobre la recogida de datos de carácter personal a través de la red[553] y, por otro lado, se insta a que se intente mantener el anonimato de los usuarios de la red[554].

Para analizar si estos portales de empleo cumplen, en primer lugar, con los principios descritos en la LOPD para el tratamiento de datos se han examinado algunos sitios webs que pueden considerarse propiamente portales de empleo[555]. En el examen realizado se observa cómo se establece un apartado en el que lo primero que se solicita, para poder inscribirse en las distintas ofertas de trabajo que gestione el citado portal, es la creación de una cuenta para después introducir el CV ya que, sin esta anotación previa, no existe ninguna opción de poder ser seleccionado por esta vía.

Respecto de los datos que se piden a la hora de cumplimentar el formulario curricular cabe valorar si es necesaria la solicitud de tanta

[552] Recomendación número R (99) 5, de 23 de febrero de 1999, sobre la protección de la vida privada en internet.
[553] Recomendación del Grupo del art. 29 2/2001, de 17 de mayo, sobre determinados requisitos para la recogida en línea de datos de carácter personal. Dictamen del grupo del art.29 sobre cuestiones de protección de datos en relación con buscadores, adoptado el 4 de abril de 2008, disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/internacional. [Consulta 20/03/2015].
[554] Recomendación del Grupo del art. 29 3/97, de 3 de diciembre, sobre el anonimato en internet.
[555] Portales de empleo analizados: www. infojobs. es, www.infoempleo.net, www. computrabajo,es, www. trabajando.com, www.monster.es www. buscojobs.es, www. netemplea.es.

información en los formularios de inscripción existentes en los portales de empleo ya que en algunos de ellos se solicita información sobre la ubicación geográfica del usuario del buscador de empleo, la dirección IP del ordenador desde el que se inscribe el solicitante de empleo o los datos sobre aficiones, etc.; lo cual no tiene relación directa con la adecuación del candidato al puesto de trabajo ofertado[556]. Desde luego que ha de entenderse que el cumplimiento del principio de calidad puede verse comprometido si, por ejemplo, se usan las direcciones de correo electrónico de los usuarios del portal de empleo para enviar comunicaciones comerciales, ya que esos datos han sido recabados con el único de fin de buscar un empleo al que se inscribe en la página web.

Por lo que, si se van a producir notificaciones de carácter comercial, se tendrá que solicitar de nuevo el consentimiento al interesado pues, en caso contrario, se estaría tratando el dato para finalidades incompatibles, es decir, no relacionadas con la consecución de un empleo. Sin embargo, no será necesario el consentimiento si esas notificaciones están relacionadas con la búsqueda de empleo, para lo cual el usuario se suscribirá en un servicio denominado "newsletter" a través del cual puede recibir informaciones de este tipo.

Esta política de privacidad, cuya finalidad principal es cumplir con el principio de información sobre el tratamiento de datos insertos en la web, a pesar de aparecer también en la página principal del buscador web de empleo pudiéndose visualizar antes de que se abra el formulario de inscripción, no suele ser consultada por la mayoría de los candidatos que, sin saberlo, pueden estar consintiendo la cesión y tratamiento de los datos de carácter personal. Sin embargo, se puede decir que la mayoría de las condiciones legales de uso de los buscadores de empleo consultados incluye un texto informativo que atiende, en mayor o menor medida, al principio de información consagrado en el art. 5 de la LOPD. A diferencia de lo que ocurre con el envío del CV a través

[556] Las denominadas *"killerquestions"*, son aquellas preguntas sobre aspectos de la vida del candidato al empleo que nada tienen que ver con su aptitud para acceder y desarrollar el trabajo. Estas preguntas pueden suponer una vulneración de la protección de datos de carácter personal, ya que estos datos, en principio, no son necesarios ni pertinentes para ser seleccionado para un puesto de trabajo.

de email, se especifican qué datos recabados son obligatorios y cuales son facultativos. En este caso, el demandante de empleo, aunque no es el que decide qué datos son los que deben aportarse al formulario web, si no cumplimenta los de carácter obligatorio no podrá acceder a los servicios del portal de empleo.

Por tanto, tal y como se establece en algunos buscadores webs, la aceptación de la política de privacidad no debe significar que el titular de los datos presta el consentimiento para que éstos sean cedidos o tratados ya que se considera que esta forma de dar el consentimiento no expresa de manera suficiente su voluntad, pues realmente no se le está informando del tratamiento que se le va a dar a esa información personal. Así pues, esta forma de prestar el consentimiento no puede ser considerada válida en el sentido de lo exige la normativa sobre protección de datos.

En cambio, otras webs de empleo establecen una casilla adicional en la que sí se específica que se solicita el consentimiento para la cesión de datos de carácter personal con fines comerciales u otros distintos a los inicialmente previstos en la recogida de la información (www.infojobs.net y www. trabajando.es). Debido a la importancia de este hecho y lo que supone la cesión de datos de carácter personal, como norma general es necesario informar sobre las posibles comunicaciones de datos insertos en ese formulario, nombrando incluso las entidades a las que van a ir destinados esos datos y, obviamente, establecer otra casilla advirtiendo de la citada comunicación. Lo que podría dar solución al cumplimiento, en primer lugar, del principio de información y, en segundo lugar, al del consentimiento, ya que si el candidato estuviera conforme marcaría esa casilla como forma de manifestar su acuerdo.

En todo caso, se deja al arbitrio del titular de los datos su cesión sin que ello deba implicar la prohibición de acceso al buscador de empleo, ya que se podría aceptar la política de privacidad pero no la cesión de los datos. Incluso se establece en las condiciones de uso de algunos buscadores webs de

empleo la posibilidad de elegir un nivel de privacidad, siendo el propio usuario el que puede restringir la cesión de los datos si pretende un nivel de confidencialidad elevado.

En la política de privacidad de los portales de empleo no se suele hacer alusión a la inscripción del fichero ante la AEPD (excepto en www.infojobs.net) por lo que no se sabe si los responsables de estos ficheros de datos cumplen con esta obligación. En muchos de los portales de empleo tampoco se dice nada sobre la legislación aplicable para la protección de datos de carácter personal, (en www.netemplea.es, en www. infojobs.net, www.trabajando.com sí que se hace alusión a la LOPD), indicándose sólo si acaso que se regirá por la normativa sobre protección de datos, sin precisar si se trata de la LOPD u otra norma[557].

Como se ha señalado antes, en los portales de empleo se suele dar la opción al demandante de empleo que inscribe sus datos en el buscador de empleo web de elegir el nivel de privacidad; por lo que indirectamente se le hace responsable del uso que se le vaya a dar a sus datos, dependiendo del nivel de privacidad que se haya establecido. Una vez más esta posibilidad se incluye dentro de las condiciones legales de uso de la página web que, como se ha dicho, no suele ser consultada por los interesados, dando lugar a una falta de transparencia sobre informaciones que pueden ser esenciales para la protección de datos de carácter personal[558].

Evidentemente, la aceptación de la política de privacidad sin conocer su contenido es responsabilidad del titular de la información incluida en la web, pero es cierto que una información tan importante tendría que advertirse de otra forma, porque de esta manera parece que lo que pretenden los proveedores de servicios webs es cumplir lo establecido en las recomendaciones sobre el tratamiento de datos en internet, sin garantizar realmente el objetivo de estas políticas que es realmente comprobar que esa

[557] www.computrabajo.es, www.monster.es, www.indeed.es.
[558] AEPD; *Selección de personal a través de internet*. 2005. pp. 20-24;

condiciones legales de uso de la página web son conocidas por los interesados que registran sus datos personales. Por ejemplo, para certificar el conocimiento de lo contenido en las políticas de privacidad, podría restringirse la utilización del buscador web a aquellos usuarios que no accedan al link informativo de la privacidad de la web.

Quizás el buscador web que menos se adapte a lo que requiere la normativa sobre protección de datos de carácter personal sea la web www. computrabajo.es. En ella se establece que se creará una base de datos con los CV enviados que podrá consultar cualquier empresa con acceso a su portal web, pero no identifica a estas empresas y tampoco solicita el consentimiento para poder realizar este tratamiento de datos. Por otra parte, menciona el derecho de cancelación instando al titular de los datos a hacer uso del mismo a través de un formulario online creado al efecto, pero añade que la web no se hace responsable si alguna empresa que haya accedido a esos datos los hubiera retenido en sus propios archivos, constituyendo este hecho, si se diera, una lesión de las garantías previstas para la cancelación, pues no se sabe el alcance que va a tener su ejercicio si esos datos han sido almacenados también en ficheros ajenos. Con esta actuación no se garantiza la protección debida en relación con el acceso al CV de los candidatos inscritos en la web, ya que otras empresas pueden hacer un uso de los datos distinto de la finalidad para la que fueron recogidos[559].

Tampoco se dice nada en estos buscadores sobre la conservación de los datos de carácter personal, es decir, no se establece el tiempo durante el cual estos portales de empleo tienen derecho a conservar los datos de las personas que se inscriben en su web, si bien la ausencia de esta información no puede conllevar ninguna sanción ya que en la propia LOPD tampoco se establece plazo, siendo la única referencia que hace a este tema la hecha a la mera posibilidad de bloquear los datos durante el tiempo necesario para cumplir con las obligaciones administrativas o judiciales que tuviera el

[559] VV.AA.: *Reclutamiento a través de internet: oportunidades y riesgos*, Harvard Deusto Business Review, 2004, pp. 64 y ss.

responsable del fichero que, en el caso de los buscadores webs de empleo, es el proveedor de servicios[560].

La política de privacidad de estos buscadores de empleo puede tener algunas carencias si se atiende a lo acordado por el Grupo del art. 29 en su Recomendación sobre determinados requisitos para la recogida en línea de datos de carácter personal[561]. Pese al criterio común de incluir en todas las condiciones de uso de la web una cláusula en la que se exponga la finalidad del tratamiento de datos, en algunos de los buscadores se deja abierta la posibilidad de que otras empresas accedan y traten esos datos, sin identificar qué empresas son y no haciéndose responsable el buscador del posible tratamiento de datos que realicen (www. infojobs.net y www. computrabajo.es). De modo que no se dice nada sobre los destinatarios de los datos cuando se produzcan cesiones, al igual que no se establece ningún listado con datos identificativos de esas otras empresas a las que se le pueden ceder ocasionalmente los datos de los demandantes de empleo inscritos en la web. Esta carencia la tienen casi todos los portales de empleo analizados, salvo en el caso de la web infoempleo en la que aparece un listado con los nombres de las empresas a las que se pueden transmitir datos con propósitos comerciales.

---

560 Tan sólo se establece un período de conservación en el citado art. 5 de la Ley 25/2007 de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (BOE núm. 251 de 19 de octubre de 2007): "*La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.2. Lo dispuesto en el apartado anterior se entiende sin perjuicio de lo previsto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sobre la obligación de conservar datos bloqueados en los supuestos legales de cancelación".*

561 Se tendrá que informar los siguientes datos: a) Identidad del responsable del tratamiento. b) Finalidad del tratamiento de datos de carácter personal. c) Obligatoriedad o no de la información solicitada y las consecuencias que tendría el titular de los datos si no la presta. d) Mención a la existencia de los derechos de acceso, rectificación, cancelación y oposición y condiciones para ejercerlo. e) Solicitud clara del consentimiento. f) Lista de destinatarios de los datos de carácter personal. g) Previsión o no de realizar un transferencia internacional de datos, especificando si es a países de la Unión Europea o no. h) Existencia de procedimientos automáticos de recogidas de datos (cookies, log, web, bugs) i)Medidas de seguridad adoptadas.

Una vez hechas estas reflexiones generales sobre la privacidad de los buscadores web, cabe atender al verdadero problema que se plantea cuando los sujetos que buscan empleados los utilizan como medio para captarlos. En este punto, es obvio que estos datos que se recogen son almacenados en las bases de datos de la propia empresa o de la empresa de intermediación que los use, constituyendo nuevos ficheros cuya responsabilidad la tendrán ahora estas entidades, situación que debería estar contemplada en la política de privacidad de las webs. Ahora bien, cuando un demandante de empleo se inscribe en la web, sus datos permanecen en su base de datos pero, si posteriormente ese desempleado se inscribe en una oferta, esa información va a ser destinada a la empresa que esté demandando el trabajo.

Por este motivo, estos buscadores se convierten también en intermediarios en el empleo y este hecho debe ser conocido por los usuarios de los mismos para que consientan o no el tratamiento de su información y la más que demostrada comunicación de datos a la empresa que ofrece el empleo. Para la cesión de datos habrá que comprobar si se dan algunas de las excepciones al consentimiento establecidas en el art. 11.2 de la LOPD para poder, entonces, justificar la falta de conformidad del demandante de empleo. Sobre este aspecto cabe decir que, si se atiende a las excepciones del consentimiento en las cesiones de datos, se puede considerar que existe la exclusión del consentimiento sólo si esa comunicación de datos es necesaria para conseguir el objetivo perseguido por la persona que se inscribe, pues para ello se hace preciso poner sus datos en conocimiento de la empresa que ofrece el empleo[562].

3.5. Descentralización y cesiones de datos realizadas por las empresas de intermediación laboral.

Como se sabe, la intermediación laboral es una actividad que propicia la ejecución de distintas cesiones de datos, las cuáles se van a describir a continuación para analizar si se realizan de la forma legalmente prevista.

[562] Art. 11.2 c) de la LOPD: "*Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique".*

En primer lugar, a la hora de seleccionar a un trabajador es muy frecuente solicitar información sobre esos candidatos de empleo a las empresas dónde previamente han desarrollado alguna actividad laboral. Es obvio que esa información no debiera ser determinante, o por lo menos no debiera constituir un criterio objetivo para contratar a un trabajador, puesto que las opiniones vertidas por otros empresarios sobre cómo ha sido el comportamiento del solicitante de empleo en su empresa pueden, a veces, ser poco objetivas o no fiables. De forma que una información negativa sobre las características profesionales o personales del demandante de empleo puede conllevar su no contratación para un concreto puesto de trabajo.

Este tipo de transmisión de información constituye, sin duda, lo que la LOPD define como cesión o comunicación de datos[563] de trabajadores para la cual se debe recoger su consentimiento. Sobre este tema, es preciso hacer alguna matización ya que se trata efectivamente de una comunicación de información pero es obvio que no se realiza con las medidas citadas y exigidas por la LOPD, puesto que, por un lado, no se tiene la conformidad de los trabajadores afectados por esos comentarios y, por otro, tampoco opera ninguna de las excepciones al consentimiento para la comunicación de datos a terceros[564].

En segundo lugar y concretamente en lo relativo al funcionamiento de las agencias de colocación, se pueden producir cesiones de datos, ya que a diferencia de las ETTs, las agencias de colocación únicamente almacenan datos para cumplir con la selección de personal encomendada y ceder esas informaciones a la empresa solicitante del servicio. Estos supuestos, deben cumplir con las exigencias establecidas para la cesión relacionadas con la prestación del consentimiento del titular del dato, al que previamente se debe haber informado de que esa actuación va a tener lugar.

---

[563] Art. 11.1 de la LOPD: *"Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado".*

[564] GOÑI SEÍN, J.L.: *El respeto a la esfera…,* op. cit., pp. 101 y ss.; FERNÁNDEZ VILLAZÓN, L.A.: "Tratamiento automatizado de datos…", op. cit., pp. 524-529; RODRÍGUEZ ESCANCIANO, S.: *El derecho a la protección de datos personales de los trabajadores: nuevas perspectivas,* Bomarzo, 2009, pág. 10.

En todo caso es la empresa que ha contratado los servicios de intermediación la que finalmente trata esos datos de forma más amplia, utilizándolos para realizar las gestiones relativas a la contratación del trabajador y para constituir un fichero con sus datos ubicados en su empresa. Las agencias de colocación se limitan integrar una primera fase de selección comunicando los datos para que la empresa cliente, que no conoce estas informaciones hasta que la agencia de colocación realiza la selección, decida finalmente sobre la contratación. En estos casos se produce una cesión de datos, regulada en el art. 11 LOPD, pero que forma parte del desarrollo de la actividad de la agencia de intermediación, por lo que no será necesaria la petición del consentimiento al titular de los datos cedidos para realizar la cesión ya que la finalidad principal de la empresa de intermediación es favorecer la contratación y la obtención de un empleo por parte de las personas que se dirigen a ella con esta pretensión[565].

Otras de las actuaciones de las agencias de colocación que puede suponer una comunicación de datos es aquella relacionada con la información que sobre su actividad deben comunicar al SEPE[566]. Pero aquí no se estaría produciendo una cesión de datos, tal y como establece la LOPD, pues esa información que se comunica no permite la identificación de ninguna persona concreta y, por tanto, se trata de datos generales sobre la actuación de las agencias de colocación.

Sobre esta concreta actividad se ha aprobado por el Consejo de Ministros un sistema de colaboración público-privada[567] en el que se incentiva económicamente a todas aquellas agencias de colocación que, entre otras actuaciones, notifiquen al SEPE irregularidades en el posible cumplimiento de

[565] FERNÁNDEZ VILLAZÓN, L.A.: "Tratamiento automatizado de datos…", op. cit., pág. 28; CARDONA RUBERT, M.B.: *Informática y contrato…,* op. cit., pág. 264 y ss.; RODRÍGUEZ ESCANCIANO, S.: *El derecho a la protección de…,* op. cit., pp. 44-45.
[566] Vid., art. 33.4 a) de la Ley de Empleo.
[567] Resolución de la Dirección General del Servicio Público de Empleo Estatal por la que se anuncia licitación de un acuerdo marco para la selección de agencias de colocación para la colaboración con los Servicios Públicos de Empleo en la inserción en el mercado laboral de personas desempleadas (BOE núm. 193 de 13 de agosto de 2013).

las obligaciones que tenga el desempleado[568]. Para poder lograr este incentivo económico (15 por ciento del pago por inserción de la persona encomendada), la información aportada por la agencia de colocación al SEPE tiene que servir para iniciarse un procedimiento sancionador contra aquel ciudadano que no ha cumplido las citadas obligaciones.

Tampoco en este caso se ha solicitado el consentimiento a los demandantes de empleo para la cesión de sus datos, pues parece más bien un control sobre el cumplimiento de sus obligaciones, premiando económicamente

[568] Art. 231.1 del Real Decreto Legislativo 1/1994, de 20 de junio, por el que se aprueba el Texto Refundido de la Ley General de la Seguridad Social (BOE núm. 154 de 29 de junio de 1994): "*1. Son obligaciones de los trabajadores y de los solicitantes y beneficiarios de prestaciones por desempleo: a) Cotizar por la aportación correspondiente a la contingencia de desempleo. b) Proporcionar la documentación e información que reglamentariamente se determinen a efectos del reconocimiento, suspensión, extinción o reanudación del derecho a las prestaciones y comunicar a los Servicios Públicos de Empleo autonómicos y al Servicio Público de Empleo Estatal, el domicilio y, en su caso, el cambio del domicilio, facilitado a efectos de notificaciones, en el momento en que éste se produzca. Sin perjuicio de lo anterior, cuando no quedara garantizada la recepción de las comunicaciones en el domicilio facilitado por el solicitante o beneficiario de las prestaciones, éste estará obligado a proporcionar a los Servicios Públicos de Empleo autonómicos y al Servicio Público de Empleo Estatal los datos que precisen para que la comunicación se pueda realizar por medios electrónicos. c) Participar en los trabajos de colaboración social, programas de empleo, o en acciones de promoción, formación o reconversión profesionales, que determinen los servicios públicos de empleo, o las agencias de colocación cuando desarrollen actividades en el ámbito de colaboración con aquéllos y aceptar la colocación adecuada que le sea ofrecida por los servicios públicos de empleo o por dichas agencias. d) Renovar la demanda de empleo en la forma y fechas en que se determine en el documento de renovación de la demanda y comparecer, cuando haya sido previamente requerido, ante la Entidad Gestora, los servicios públicos de empleo o las agencias de colocación cuando desarrollen actividades en el ámbito de colaboración con aquéllos. e) Solicitar la baja en las prestaciones por desempleo cuando se produzcan situaciones de suspensión o extinción del derecho o se dejen de reunir los requisitos exigidos para su percepción, en el momento de la producción de dichas situaciones. f) Reintegrar las prestaciones indebidamente percibidas. g) Devolver a los servicios públicos de empleo, o, en su caso, a las agencias de colocación cuando desarrollen actividades en el ámbito de colaboración con aquéllos, en el plazo de cinco días, el correspondiente justificante de haber comparecido en el lugar y fecha indicados para cubrir las ofertas de empleo facilitadas por los mismos. h) Inscribirse como demandante de empleo, mantener la inscripción y cumplir las exigencias del compromiso de actividad en los términos establecidos en el artículo 27 de la Ley 56/2003, de 16 de diciembre, de Empleo.i) Buscar activamente empleo, participar en acciones de mejora de la ocupabilidad, que se determinen por los servicios públicos de empleo competentes, en su caso, dentro de un itinerario de inserción. Los beneficiarios de prestaciones acreditarán ante al Servicio Público de Empleo Estatal y los Servicios Públicos de Empleo autonómicos, cuando sean requeridos para ello, las actuaciones que han efectuado dirigidas a la búsqueda activa de empleo, su reinserción laboral o a la mejora de su ocupabilidad. Esta acreditación se efectuará en la forma en que estos organismos determinen en el marco de la mutua colaboración. La no acreditación tendrá la consideración de incumplimiento del compromiso de actividad. Sin perjuicio de acreditar la búsqueda activa de empleo, la participación en las acciones de mejora de la ocupabilidad que se correspondan con su profesión habitual o sus aptitudes formativas según lo determinado en el itinerario de inserción será voluntaria para los beneficiarios de prestaciones contributivas durante los treinta primeros días de percepción, y la no participación en las mismas no conllevará efectos sancionadores".*

a las agencias de colocación que firmen el convenio si finalmente se comprueba dicho incumplimiento por parte del trabajador.

Respecto a las cesiones de datos que se producen en la agencia de recolocación hay que atender a una doble perspectiva; Por un lado, se establece una comunicación de datos de la empresa que despide al trabajador a la agencia de recolocación y; por otro, de la agencia de recolocación a la empresa que aspira a contratar a ese trabajador. Para la primera cesión es imprescindible que opere el consentimiento del trabajador despedido ya que la relación contractual con la empresa ha terminado y ésta no va a colaborar en ninguna de las funciones de la empresa de recolocación ya que ese trabajador no va a ser colocado ninguno de sus centros de trabajo. Por su parte, la agencia de recolocación establece una nueva relación con el trabajador despedido pues, antes, esos datos del trabajador pertenecían al empresario, el cual tenía la condición de responsable del fichero y, ahora, pasan a estar en ubicados en ficheros cuya responsabilidad es de la agencia. Para el segundo supuesto de cesión, de la agencia de recolocación a la empresa que va a contratar al demandante de empleo, se entiende que también sería necesario el consentimiento ya que la agencia de recolocación tan sólo pone en contacto a los desempleados con las empresas que ofrecen empleo, sin realizar una selección previa de candidatos, función que le corresponde estas empresas, siendo ellas las que finalmente deciden sobre su capacidad profesional y posterior incorporación a la empresa.

Por último, cabe citar las cesiones de datos que operan en el ámbito de actuación de las ETTs, ya que no queda del todo claro que la empresa usuaria tan sólo deba limitarse a conocer la información relativa a la aptitud profesional del candidato, sobre todo teniendo en cuenta que ese trabajador se tiene que someter a las pautas de organización y dirección de ese empresario. Aunque, en la práctica, la cesión de estos datos es mínima[569], es cierto que, además de

[569] Art. 17 del RD 417/2015: "*Las empresas de trabajo temporal están obligadas a remitir por medios electrónicos al Registro de Empresas de Trabajo Temporal de la autoridad laboral competente, dentro de los primeros diez días de cada mes y en el modelo que se establezca en las disposiciones de desarrollo de este real decreto, una relación de los contratos de puesta a disposición celebrados en el mes anterior, en la que deberá constar: a) Nombre, número de*

la información contenida en el contrato de puesta a disposición[570] , se debería de otorgar a la empresa usuaria la facultad de averiguar otros datos siempre que estén relacionados con el desempeño de la tarea a encomendar .En este sentido, las ETTs tendrán que informar al candidato al empleo del destino y finalidad que se le va a dar a esos datos[571], advirtiendo que no sólo van a ser utilizados para el proceso de selección sino que se utilizarán también para hacer las gestiones referidas a su contratación, si es seleccionado y finalmente acepta el puesto de trabajo.

Evidentemente, todas estas agencias de intermediación pueden pedir la colaboración de una empresa externa para realizar gestiones relacionadas con la selección de personal[572]. En estos supuestos se estaría realizando una cesión de los datos para que ésta segunda empresa pudiera tratarlos, siendo la que ostenta la condición de encargada del tratamiento. A estos efectos, esta empresa externa tendrá que formalizar un contrato con la empresa de intermediación atendiendo a lo establecido en los arts. 12 LOPD y 20 del RDLOPD en relación con el llamado contrato de hospedaje[573].

---

identificación fiscal y código de cuenta de cotización a la Seguridad Social de los centros de trabajo de las empresas usuarias. b) Número de contratos celebrados con cada una de ellas, desglosado por supuestos de celebración, de conformidad con lo previsto en el artículo 6.2 de la Ley 14/1994, de 1 de junio. c) Número total de trabajadores puestos a disposición de las empresas usuarias. Si un trabajador hubiera sido cedido en más de una ocasión, a la misma o distinta empresa usuaria, se computará una sola vez. Dicha documentación se remitirá igualmente en el caso de que la empresa no haya formalizado contratos de puesta a disposición, haciendo constar tal circunstancia".

[570] Acerca del contenido del contrato de puesta a disposición vid., VALDÉS DAL-RE, F.: "Contrato de puesta a disposición entre empresa de trabajo temporal y empresa usuaria", en VV.AA.: Comentarios a la Ley de Empresas de Trabajo Temporal, La Ley, 2009, pp. 231-235; GONZÁLEZ ORTEGA, S. Y GÓMEZ-MILLÁN HERENCIA, M.J.: "Forma y…", op. cit., pp. 119-120.

[571] Este derecho a la información no es absoluto puesto que tal y como se establece en el art. 5.3 de la LOPD no será necesaria la información cuando su contenido se deduzca claramente de las circunstancias en las que se recaben los datos o la naturaleza de los mismos.

[572] Los supuestos en los que las empresas de intermediación pueden realizar el encargo del tratamiento de datos pueden ser; gestión de seguridad social, formación, envío de documentación, elaboración de la nómina por gestorías externas etc.

[573] Art. 12.2 de la LOPD; *" La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar."* Art. 20.2 y 3 del RDLOPD; *"Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este Capítulo deberá velar por que el*

En el contrato de hospedaje se debe dejar claro que este tercero encargado del tratamiento no comunicará los datos a otras personas ajenas a su empresa ni siquiera para su conservación, es decir, el responsable del fichero, empresa de intermediación, debe saber en todo momento dónde se encuentran los datos facilitados por el demandante de empleo[574]. Es posible que ese tratamiento de datos se realice en los soportes informáticos de la empresa contratada para colaborar en la gestión de los recursos humanos. Si esto ocurre, esta empresa externa, en cuanto encargada del tratamiento, tendrá que adaptar su sistema para poder implantar las correspondientes medidas de seguridad de los datos, las cuáles deben quedar recogidas en el contrato de hospedaje[575].

Ahora bien, si el encargado del tratamiento utiliza los datos de carácter personal para una finalidad distinta, o no cumple con lo establecido en el contrato, y tampoco observa diligentemente las medidas de seguridad impuestas, será considerado también responsable del tratamiento[576] pues se

---

encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente. No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente Capítulo".

[574] Según la AEPD: "*En primer lugar, es preciso que el acceso a los datos por el tercero se efectúe con la exclusiva finalidad de prestar un servicio al responsable del fichero, y que dicha relación de servicios se encuentre contractualmente establecida. En lo que atañe a los requisitos formales de este tipo de contratos, el artículo 12.2 impone que "la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas".* Vid., Informe jurídico 513/2004 de la AEPD.

[575] DAVARA FERNÁNDEZ DE MARCOS, I.: *Hacia la estandarización de la…,* op. cit., pp. 268-271.

[576] GONZÁLEZ TAPIA, M.L: "España: El encargado del tratamiento de datos" *AR: Revista de derecho informático*, núm. 110, 2007, pp. 40-44; AEPD: *Guía del responsable del Fichero*. 2008, pp. 30-31; APARICIO SALOM, J.: *Estudio sobre la Ley…,* op. cit., pp. 41-43; APDCM: *Principios y derechos de la protección de datos de carácter persona*l, Thomson Civitas, 2010, pp. 561-564; VV.AA.: "La protección de datos de carácter personal" *Edición digital Aranzadi*, 2014, pp. 8-12.

habrá extralimitado en el desarrollo de la tarea encomendada[577]. Sobre este aspecto la jurisprudencia ha atribuido la responsabilidad del fichero al encargado del tratamiento, como consecuencia de la falta de observancia de las pautas establecidas en el contrato de hospedaje[578].

3.6. Cumplimiento de las exigencias relacionadas con la protección de datos por los instrumentos informáticos que colaboran con la intermediación laboral.

Como ya se ha comentado, en la intermediación laboral se puede disponer de una serie de herramientas informáticas para colaborar en los procesos de búsqueda de empleo que se gestionan. Lógicamente, en estos mecanismos también se producen tratamientos de datos, siendo el más común y directo el almacenamiento, pues estas plataformas webs recepcionan la información que incluyen los demandantes de empleo. También en este aspecto se tendrá que analizar lo establecido en su política de privacidad o en las condiciones legales de uso, para constatar de esta forma el cumplimiento de las obligaciones marcadas por la normativa sobre protección de datos de carácter personal. Para ello, no se va a hacer una descripción detallada del contenido de las políticas de privacidad de estos sistemas, sino que, más bien, se va a atender a las particularidades que se puede presentar, ya que en muchos aspectos suelen coincidir todas.

3.6.1. Intermediación pública, Tics y datos de carácter personal.

Sobre los medios informáticos adheridos al SNE se puede decir que, por ejemplo, en la web empléate se producen, de forma continua, remisiones a otros portales y se establece una cláusula sobre protección de datos cuya descripción es bastante escueta[579]y que curiosamente hace alusión a que el

[577] Art. 12.4 de la LOPD; *"En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente".*

[578] Vid., Sentencia de la Audiencia Nacional de 18 de octubre de 2007 (JUR 2007\346177).

[579] Política de privacidad sede electrónica del SEPE, disponible en https://www.sepe.es/contenidos/enlaces_pie/aviso_legal.html: *"La política de privacidad de la Web se basa en: Datos imprescindibles. La solicitud exclusivamente de los datos imprescindibles para poder proporcionarle los servicios de la Web. Derechos de acceso, rectificación, cancelación u oposición. En todo el momento la persona usuaria podrá ejercer los*

responsable del fichero no es el SNE, del que depende este portal, sino el SEPE o los SEP autonómicos. Con este aviso legal se vuelve a confirmar que las gestiones relacionadas con la información personal de los demandantes de empleo la tienen aquellos servicios con competencias en la intermediación laboral (SEP autonómicos), pues en este ámbito público es dónde mayores tratamientos de datos se realizan para lograr así un cumplimiento efectivo de su labor como ejecutores de las políticas activas de empleo.

Ahora bien, como paso previo para poder acceder a estos servicios –web empleate-, es necesario el registro del candidato al empleo en la plataforma empléate, para lo cual, al igual que ocurre con los buscadores web de empleo del ámbito privado, el interesado tiene que marcar la casilla de aceptación de la política de protección de datos. Esta política de privacidad presenta grandes carencias ya que no informa ni del objetivo de la web, ni dice nada sobre la posible cesión de datos, ni tampoco del requerimiento del consentimiento al titular del dato para que ésta se pueda efectuar.

Además de esto, es muy importante que las gestiones efectuadas en la sede electrónica se realicen por los sujetos interesados pues, tal y como ha

---

derechos de acceso, rectificación, cancelación u oposición ante la Subdirección General de Estadística e Información del Servicio Público de Empleo Estatal. Información técnica imprescindible. El Servicio Público de Empleo Estatal recabará la mínima información técnica imprescindible para ofrecer un buen servicio a través de esta Web. En particular, cuando la persona usuaria se conecta a la Web, el Servicio Público de Empleo Estatal analiza exclusivamente el tipo de navegador utilizado y su versión, con el objetivo de seleccionar la hoja de estilo más adecuada y que la visualización de la Web sea correcta, así como el idioma y el juego de caracteres de su navegador con el mismo motivo, como por ejemplo, para la correcta visualización de caracteres acentuados. El Servicio Público de Empleo Estatal podrá utilizar "cookies" para almacenar información de personalización de usuarios y usuarias. En todo caso, si la persona usuaria de la Web no desea aceptar la grabación de la "cookie" en su ordenador, podrá navegar por la Web sin ningún tipo de restricción. Recogida de datos estadísticos. La utilización de "cookies" de visita se podrá emplear con fines estadísticos (en concreto, conocer el número de "visitantes únicos" que acceden a la Web) no almacenando más información que un número de 128 bits generado aleatoriamente. Con la finalidad de ofrecerle el mejor servicio a través de esta Web, y con el objeto de facilitar su uso, se analizan el número de páginas visitadas, el número de visitas, así como la actividad de las personas visitantes de la web, y su frecuencia de utilización. Con esta información se analiza la frecuencia de uso de la Web del Servicio Público de Empleo Estatal a partir de los datos de conexión, y las secciones más visitadas. Enlaces con otras páginas. Esta política de privacidad sólo es de aplicación a la Web del Servicio Público de Empleo Estatal, no se garantiza en los accesos a través de enlaces con este sitio, ni a los enlaces desde este sitio con otras webs".

previsto la AEPD[580], resulta sencillo acceder a estos servicios con la simple introducción del DNI, el cual puede ser conocido por alguna persona ajena a la gestión de datos identificativos y profesionales del interesado, incumpliendo el responsable del fichero -Subdirección General de Tecnologías de la Información y Comunicaciones- con las medidas de seguridad pertinentes.

Como consecuencia de las gestiones realizadas en la web del SNE se genera un documento electrónico[581] que tiene la misma validez que cualquier escrito que sea expedido físicamente por la Administración. Por este motivo, es importante certificar la protección de la información introducida en esta categoría de documentos, pues también existe la posibilidad de imprimirlos en formato papel. Sobre este tema, el RDLOPD[582] establece que las copias de estos documentos tendrán que ser supervisadas por la persona autorizada en el documento de seguridad, es decir, que, aunque el documento permanezca en la base de datos de la sede electrónica del SNE, la responsabilidad generada por las posibles copias del mismo también recaerá sobre el responsable de ese fichero electrónico, el cual tendrá que velar por la implantación de las medidas de seguridad pertinentes para que ningún tercero pueda disponer y hacer copias de esos documentos. En este sentido, el titular de los datos es el sujeto que puede acceder a esos documentos en la medida en que puede entrar en el perfil en la sede electrónica a través de usuario y contraseña o de certificado digital[583].

---

[580] Resolución de la AEPD R/02714/2009, disponible en http://www.agpd.es/ portalwebAGPD /resoluciones/admon_publicas/ap_2009/common/pdfs/AAPP-00055-2009_Resolucion-de-fecha-14-12-2009_Art-ii-culo-5-9-y-10-LOPD.pdf [Consulta 20/12/2014].

[581] Art. 30 de la LAECSP: "*Las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las Administraciones Públicas, manteniéndose o no el formato original, tendrán inmediatamente la consideración de copias auténticas con la eficacia prevista en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que el documento electrónico original se encuentre en poder de la Administración, y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento."*

[582] Art. 11 del RDLOPD: "*1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad. 2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior".*

[583] VALERO TORRIJOS, J.: "Implicaciones para la protección de datos de carácter personal de la Administración Electrónica" en VV.AA.: *La protección de datos en la Administración Electrónica*, Aranzadi-Thomson Reuters, 2009, pp. 190-194.

También en las oficinas virtuales de empleo de las CCAA se producen, lógicamente, tratamientos de datos de aquellos desempleados que acuden a ellas para encontrar un empleo. Al igual que ocurre con los servicios de la web del SNE, los usuarios que quieran utilizar las prestaciones de la oficina virtual de empleo tendrán que aceptar lo establecido en la política de privacidad, autorizando con este hecho la utilización de sus datos personales, formativos y curriculares, con la intención de que permanezcan en la red y sean consultados a través de medios electrónicos.

En estos portales de empleo autonómicos, como regla general, la información sobre la privacidad de los datos se proporciona con cierta parquedad y tan sólo se insta al titular de los datos a consultar la LOPD, informando de que esa es la normativa por la que se rige la web. Es decir, se anuncia simplemente la existencia de una norma protectora de la información personal, pero nada se dice de su contenido y, por tanto, se coloca al demandante de empleo en una situación de indefensión, pues evidentemente no tiene por qué conocer el alcance de la normativa sobre protección de datos de carácter personal ni los derechos que tiene[584]. De hecho, un candidato a un empleo se puede inscribir en una oferta de empleo enviando su CV al email de la oficina de empleo que lo gestiona sin que se le proporcione información sobre la finalidad o la utilización que se le va a dar a los datos insertos en su CV o, también, se puede inscribir en el portal de empleo a través de la cumplimentación de una serie de datos, siendo en este supuesto dónde la información sobre la aplicación de la LOPD es más amplia[585].

---

[584] En la web del Servicio Andaluz de Empleo (*http://www.juntadeandalucia.es/servicio andaluzdeempleo/web/websae/portal/es/index*.) a la hora de publicar ofertas de empleo aparece una leyenda en la que la persona que ofrece el puesto de trabajo se compromete a *" En cumplimiento de lo establecido en la LOPD, declaro bajo mi responsabilidad que los datos de los curriculums de las personas candidatas facilitados por el SAE a través de la oficina virtual de empleo, se utilizaran exclusivamente en la gestión del proceso de selección para la cobertura de los puestos de trabajo ofrecidos, no comunicándolos a otras personas y, procediendo a la destrucción de los mismos; al igual que cualquier soporte o documento en los que conste algún dato de carácter personal de las personas candidatas, una vez cumplida la finalidad para la cual se han solicitado".*

[585] En el portal de empleo de Asturias se establece una leyenda en la que se informa de los siguientes aspectos: *"De acuerdo a lo establecido en el artículo 5 de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal se informa; a)De la existencia de un fichero o tratamiento de datos de carácter personal cuya finalidad*

En todos estos supuestos es necesario también considerar si se cumple con el principio de consentimiento, aunque puede afirmarse que en los portales de empleo autonómicos no se refleja de forma clara esa exigencia del consentimiento para el tratamiento de los datos personales. Esto es así por cuanto el consentimiento sólo se solicita al titular de los datos con la finalidad de realizar un posible tratamiento consistente en la facultad de ceder los datos de los demandantes de empleo a otras empresas, para cumplir así con la finalidad de búsqueda de trabajo[586], atendiendo de esta manera a su funcionalidad como intermediario laboral, pero nada se dice de qué empresas son las que van a recibir esos datos. Ciertamente, resulta llamativo que, tratándose de la misma norma para ambos supuestos –públicos y privados-,/estos portales de empleo contengan una política de privacidad tan poco clara, mientras que en otros buscadores de empleo privados, como se ha visto, sí se establezca de forma más precisa la manera de proteger esos datos.

A modo de ejemplo, y como muestra del incumplimiento de la LOPD en el tratamiento de datos de carácter personal realizado por los SE autonómicos, y más concretamente del principio de seguridad de los datos, la AEPD ha resuelto una denuncia presentada contra el SAE en relación con el hecho de que al solicitante de empleo se le asigna un número para la cita que pide a

---

es proporcionar una herramienta de utilidad en la búsqueda de empleo y cuyos destinatarios son las personas que crean sus propios usuarios y contraseñas de acceso a este servicio proporcionado a través de la web Trabajastur. b) El suministro de los datos es de carácter voluntario. c) Usted podrá ejercitar sus derechos de acceso, rectificación, cancelación y oposición sobre los datos tratados contactando con el correo electrónico spempleo@asturias .org/Administración de Trabajastur"

[586] Privacidad del Servicio de Ocupación Catalán; "*De conformidad con las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, le informamos que los datos que usted proporciona en el SOC a través de los formularios de estas páginas, serán incorporados a un fichero que el SOC es responsable con el fin de realizar la intermediación entre empresas y candidatos. El uso del Portal a los efectos de diferentes intermediarios, para lo cual se ha creado lo puede ser debido a la baja para empresas y candidatos. Los datos de los formularios indicados con un asterisco son obligatorios y su ausencia será la gestión de la correduría. Podrá ejercitar sus derechos de acceso, cancelación, rectificación y oposición en la forma legalmente establecida, enviando una carta al SOC, adjuntando una copia de su DNI/NIE. Registro en el Servei d' Ocupació de Catalunya. usuarios de trabajo activo que desean aplicar para cualquier otro servicio del SOC tendrán que inscribirse como demandante de empleo en su oficina."* Portal del Servicio Andaluz de empleo, cita que aparece cuando se envía el CV a una oferta publicada; *"Declaro que los datos por mí aportados a la Oficina Virtual de Empleo, son verdaderos que podré acreditarlos cuando así me lo soliciten y doy mi consentimiento para que el SAE los facilite a aquellas empresas que realicen procesos de intermediación a través de este portal".*

través de la plataforma virtual del SAE y, cuando se dirige a una de las oficinas del SAE, encuentra su número en el tablón electrónico seguido de su DNI y de la hora en la que tenía cita previa, pudiéndolo identificar de esta forma cualquier persona que estuviera en la oficina de empleo.

Sobre este hecho, la AEPD, aunque acordó no iniciar procedimiento administrativo sancionador, sí reconoció que se estaba incumpliendo la normativa sobre protección de datos utilizándolos para fines distintos de los establecidos ya que terceras personas ajenas a los servicios del SAE estaban identificando a una persona ubicándola en la citada oficina de empleo. La AEPD, aunque, como se ha dicho, no inició un procedimiento sancionador, sí consideró oportuno recomendar la implantación de sistemas que garanticen un mayor nivel de confidencialidad, estableciendo medios que identifiquen a las personas emplazadas para cursar trámites mediante las iniciales del nombre y apellidos junto a un número[587].

En cuanto al cumplimiento de las exigencias relativas a la protección de datos por parte del SISPE, como base de datos que pone en relación el SEPE y los SE autonómicos, es claro que los desempleados tienen que estar debidamente informados sobre la finalidad de esta gran base de datos (SISPE) y prestar su autorización para las posibles cesiones que se puedan dar en el marco de su actuación como herramienta de colaboración con la intermediación laboral pública.

Existe un clara diferenciación entre este servicio y las oficinas virtuales de empleo en lo relativo al acceso a los datos de carácter personal ya que el SISPE se presenta como una herramienta de trabajo interna[588] para poner en relación a los distintos SEP autonómicos con el SEPE, al igual que realizan estadísticas mensuales sobre las colocaciones y los datos sobre población

[587] A pesar de esta recomendación de la AEPD, este sistema se sigue utilizando en la oficina de empleo del SAE, haciendo caso omiso a las advertencias realizadas por la AEPD (Fuente: Consulta realizada a los funcionarios de la oficina del SAE sita en C/ José María Sánchez Bedoya, Sevilla).
[588] Al ser el SISPE una herramienta de trabajo interna, serán los funcionarios los que deberán estar informados y formados acerca del tratamiento de datos que debe realizarse.

desempleada, las cuales constituyen un censo que sirve para orientar a los distintos SPE. El modo de proceder en las oficinas virtuales de empleo es diferente puesto que se ofertan una serie de servicios a los que el ciudadano accede directamente con el certificado digital con el fin de agilizar las gestiones ante el SEPE.

En este caso, los usuarios deben saber que sus datos van a ser gestionados en el SISPE y conocer, en todo caso, la identidad del responsable del fichero para poder ejercer los derechos de acceso, rectificación, oposición y cancelación. En este sentido, con la informatización de los datos de los desempleados en una base común como es el SISPE, se ha producido un acceso a los datos desde los sistemas informáticos mucho más generalizado ya que, en la configuración de los ordenadores de trabajo de los distintos SEPE, se instalan estos sistemas informáticos para todos los trabajadores, si bien sólo tendrán acceso a esa herramienta las personas a quienes se le haya dado previamente un usuario y contraseña, autorizados, por tanto, para efectuar cualquier utilización de los datos dirigida por el responsable del fichero para la que tendrán que cumplir las exigencias de la normativa sobre protección de datos.

Si se tuvieran que ceder datos insertos en el SISPE, se podría excepcionar el consentimiento del interesado que, siendo conocedor de estas actuaciones, ha aceptado previamente la política de privacidad de la web del servicio público de empleo en la que ha incluido su información, la cual, si está correctamente creada, debe hacer alusión a la existencia del SISPE y a las gestiones derivadas de su actuación. De todas formas, aunque el titular del dato no conociera la presencia del SISPE porque no se le hubiera informado mediante la política de privacidad, la comunicación de datos se puede realizar sin el consentimiento de su titular siempre que tenga como objeto la transmisión de información entre las distintas administraciones con el fin de

realizar estadísticas de empleo, tal y como establece el art. 11.2 e) de la LOPD[589].

Para que las agencias de colocación puedan acceder a este sistema de transmisión de datos o Espacio Telemático Común[590], tendrán que tener un usuario y una clave que les será proporcionada por el SEPE, siempre que previamente la agencia haya sido autorizada. Una vez que la agencia de colocación introduce su código y contraseña puede empezar a introducir información de sus usuarios en el ETC. En un primer momento, los datos que se van a incorporar a la información integrada del SISPE son los relacionados con el número de personas atendidas, para, en un momento posterior, introducir datos, no sólo referidos al primer contacto que éste haya tenido con la agencia, sino otros relacionados también con el resto de actividades realizadas para la posible colocación del candidato y con la consecución de este objetivo si se hubiera conseguido. En esta línea, también se pueden aportar datos concernientes a colectivos con dificultades de inserción, personas con discapacidad, o los que tienen que ver con la nacionalidad del demandante de empleo[591].

Si se atiende a lo establecido en la LOPD, se puede observar cómo estos datos, que maneja la agencia de colocación y que transmite al SISPE, son evidentemente datos de carácter personal, en particular si se identifica concretamente a algún desempleado, teniendo algunos, incluso, la categoría

[589] Art. 11.2 e) de la LOPD: "Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos".

[590] En este espacio se intercambia la siguiente información, expresada en el art. 6 del RD 1796/2010: *"1. Comunicar electrónicamente las autorizaciones concedidas para constituirse como agencia de colocación. 2. Acceder a la relación actualizada de agencias de colocación autorizadas por los distintos servicios públicos de empleo, al objeto de que pueda ser conocida tanto por los servicios públicos de empleo como por la ciudadanía. A estos efectos, esta relación estará disponible en las webs de dichos servicios públicos de empleo.3. Realizar el suministro de información periódica establecido en el artículo 5.m). 4. Cumplimentar la Memoria anual contemplada en el artículo 5.n). 5. Aportar, por las agencias de colocación que tengan suscrito convenio de colaboración con los servicios públicos de empleo, la información resultante de su gestión, cumpliendo los protocolos establecidos en el Sistema de Información de los Servicios Públicos de Empleo, en cuanto a contenidos y procesos de consolidación de la información".*

[591] Sistema Nacional de Empleo: *Agencias de colocación. Espacio Telemático Común*, Ministerio de Empleo y Seguridad Social, 2015. pp.3-5, 16-21, disponible en: http://www.sistemanacionalempleo.es/pdf/agencias/instrucciones_envios.pdf.

de datos especialmente protegidos (colectivos con dificultades de inserción, personas con discapacidad, etc.). Como es lógico, cuando la agencia de colocación recoge la información de los demandantes de empleo, deberá informar a los titulares de esos datos del uso y destino que van a tener, así como del tratamiento y las posibles cesiones que se vayan a realizar, tal y como establecen los arts. 5 de la LOPD y 8 del RD 1796/2010[592].

Así pues, la comunicación de datos a través del ETC debe ir precedida del consentimiento de los titulares de esos datos, pues el simple acto de ceder los datos supone un tratamiento de información personal, aunque este consentimiento podrá ser exceptuado si esa cesión se realiza sólo entre administraciones públicas para fines estadísticos, científicos e históricos. En todo caso, si la comunicación de datos versa sobre datos especialmente protegidos, la LOPD establece que ese consentimiento ha de ser expreso.

En este contexto, es conveniente analizar algunas políticas de privacidad de las agencias de colocación, sobre todo para comprobar si cumplen con el principio de información contenido en la LOPD y en el RD 1796/2010, pudiéndose percibir que esos datos se utilizan para las funciones de la agencia descritas en el RD 1796/2010, pero nada se dice sobre su transmisión a través del ETC al SISPE. Tampoco exponen de forma clara y precisa las funciones de la agencia y el destino que se le va a dar a estos datos, ni tampoco si son colaboradoras del SEPE y qué contenido tiene el convenio de colaboración establecido con ellos[593].

Esta ausencia de información en la web de la agencia de colocación, respecto al uso y tratamiento de datos allí contenidos, conlleva una infracción catalogada como leve en el art. 44.2 de la LOPD. El encargado de cumplir con

[592] Art. 8 del RD 1796/2010; *"Las personas que se inscriban como demandantes de empleo tendrán derecho a ser informadas por los servicios públicos de empleo sobre las agencias de colocación autorizadas que operan en su territorio, así como que dichas agencias no podrán exigirles ninguna contraprestación por su actuación".*

[593] Ejemplos de agencias en las que no existe información detallada sobre el destino que la agencia otorga a los datos de carácter personal; http://www.interempleo.es/politica-privacidad; http://www.acpgranada.com/index.php/agencia-de-colocacion;http://www.dplett.com/ETT-AVISOLEGAL.pdf. [Consulta 1/12/2014].

esta obligación de información y destinatario de la infracción, en el caso de que no la ejerciera, es la propia agencia de colocación pues es la responsable del fichero de datos que se cree con la información dada a través de la web y, por tanto, tiene la misión de informar sobre el destino y uso que se le va a dar a esos datos.

Sobre esta cuestión se puede decir que en la normativa que regula las agencias de colocación – RD 1796/2010- no se regula el acceso que tendrán los ciudadanos al ETC, sino que se trata más bien de una exposición del significado y sentido de la plataforma sin mencionar ninguna instrucción sobre qué requisitos tienen que cumplir los usuarios de los servicios ofrecidos por el ETC[594]. Por este motivo, el ETC se concibe, más bien, como un programa interno de trasvase de información para facilitar una eficaz intermediación laboral, poniendo en contacto a todos los agentes públicos dedicados a gestionar políticas activas de empleo. A la hora de establecer exigencias de seguridad en las relaciones que, a través de plataformas de intercambio de datos, tienen las agencias de colocación, sobre todo en lo concerniente a la transmisión de datos a través del ETC, es necesario atender lo que dice la LOPD y el RDLOPD sobre los niveles de protección –básico, medio y alto[595]- y las posibles sanciones que existen en caso de incumplimiento de las medidas de seguridad[596].

3.6.2. Utilización de programas informáticos y su repercusión sobre el derecho a la protección de datos.

Como es sabido, existen sistemas inteligentes que colaboran en las tareas de selección de personal consistentes en poner en relación rasgos de la personalidad de los posibles candidatos al empleo. El problema es que, a

[594] SOBRINO GONZÁLEZ, G.: "Régimen jurídico de las agencias de colocación", *Revista Temas Laborales* núm. 110, 2011, pp. 60-62; TOSCANI GIMÉNEZ, D.: "El nuevo marco legal de los servicios de colocación y empleo. Especial referencia a las agencias privadas de empleo y empresas de trabajo temporal tras la reforma laboral de 2010" *Revista de Trabajo y Seguridad Social,* CEF, núm. 335, 2011, pp. 129-170; RODRÍGUEZ ESCANCIANO, S: *La intermediación en el mercado…,* op. cit., pp. 376-377.
[595] Vid., art. 80 y 81 del RDLOPD.
[596] Art. 44.3 h) de la LOPD: "*h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".*

partir de ese tratamiento de datos, se pueden averiguar informaciones que nada tienen que ver con la valoración de la capacidad profesional del demandante de empleo, por lo que su obtención, sin haberlas solicitado previamente, derivadas de los resultados de los tests psicológicos que realiza Sigmund, no cumple con el principio de calidad o pertinencia en el tratamiento de datos.

La aplicación de estos sistemas es algo que se admite en la práctica, pero realmente con su realización se llegan a conocer más datos del solicitante de empleo que pueden no ser esenciales para el desarrollo del proceso de selección de personal. Tampoco se cumple con el principio de información porque el titular del dato no conoce la verdadera finalidad del sistema. Por tanto, el consentimiento que presta el demandante de empleo no es válido ya que no va precedido de la información por parte del sujeto que va a tratar los datos con un objetivo distinto del meramente relacionado con la realización de un proceso de búsqueda de empleo que cumpla todas las garantías previstas en la normativa sobre protección de datos[597]. Para intentar adecuar como mecanismo de selección de personal la realización de los test que propone Sigmund, se tendría que delimitar, entonces, la información que obtiene el empresario a través de estos sistemas, por ejemplo, haciendo test específicos para el puesto ofertado que valoren las características técnicas del candidato para la realización de la tarea que vaya a desempeñar en la empresa, cumpliendo así el principio de proporcionalidad para el almacenamiento y tratamiento de esos datos[598].

Ahora bien, siguiendo lo ordenado en la LOPD para las comunicaciones de datos a terceros[599], se pueden dar aquí dos supuestos: el primero, relacionado con la simple adquisición del software sin que ese tercero llegue a conocer ningún dato de los introducidos en el mismo y, el segundo, el referido a

[597] BOURCIER, D.: *Inteligencia artificial y derecho*, Ed. UOC, 2003, pág. 148; PORRET GELABERT, M.: *Manual para la gestión del capital humano en las organizaciones*., ESIC editorial, 2014, pp. 84-89; VV.AA. "Sistema experto para la selección de personal desarrollador de software" *Ingenio Magno,* vol. 4, pp. 75-81.
[598] FERNÁNDEZ DOMÍNGUEZ, J.J. Y RODRÍGUEZ ESCANCIANO, S.: *Utilización y control de datos…*, op. cit., pp. 115-117.
[599] Vid., art. 11.1 de la LOPD.

la posibilidad de que este tercero sea el que gestione y controle el programa. En el segundo caso, se estaría comunicando la información de los candidatos de empleo, convirtiéndose la empresa del software en encargada del tratamiento y, por tanto, obligada a cumplir con las especificaciones contenidas en el contrato de hosting (art. 12 LOPD). Aun así, la obligación de inscribir el fichero de datos que se cree, en el marco de este contrato de hosting, la tendrá el responsable del fichero, pues es el que en primera instancia recoge los datos de los demandantes de empleo.

Puede ocurrir que las empresas de intermediación contraten los servicios de almacenamiento de los datos de los solicitantes de empleo con una empresa externa. En este caso, también se debe redactar el citado contrato de hosting que cumpla con los requisitos del art. 12 de la LOPD[600]. De esta manera, se podrá acceder a estos datos desde cualquier soporte informático con conexión a internet, siendo la empresa prestadora de servicios de cloud computing la encargada del tratamiento, la cual tan sólo podrá realizarlo siguiendo las instrucciones de la empresa de intermediación que contrate sus servicios, siendo ésta la responsable del fichero[601]. Es así como el responsable del fichero tiene que velar porque se cumpla la normativa de protección de datos[602]. Ahora bien, si el encargado del tratamiento no la cumple o hace un uso de los datos con una finalidad distinta de la acordada sin que el responsable del fichero tenga conocimiento de ello, incurrirá en las mismas infracciones que si lo hubiera realizado el responsable del fichero[603], es decir, una infracción grave a tenor de lo dispuesto en el art. 44.3 c) de la LOPD[604].

---

[600] Art. 12.2 de la LOPD: *"La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar".*

[601] AEPD: *Orientaciones para prestadores de servicios de cloud computing*, 2013, pp. 5-6.

[602] MARZO PORTERA, A.: "Privacidad y cloud computing, hacia dónde camina Europa", *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche*, Vol. I, núm. 8 , 2012, pp.202-229.

[603] Art. 20. 2 y 3 del RDLOPD: *"2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este Capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento. 3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las*

El problema principal que acarrea el uso de estos sistemas de almacenaje online es la pérdida del control efectivo sobre la ubicación física de los datos, propiciada por la propia naturaleza del sistema, pues se permite que estos datos puedan estar situados en cualquier parte del mundo. Este puede ser uno de los inconvenientes del cloud computing lo que contribuye a que muchas empresas de selección de personal no contraten estos servicios debido a la incertidumbre que genera el no saber si sus datos están seguros y si se cumplen sus parámetros de confidencialidad; sobre todo teniendo en cuenta que estas agencias deben cumplir sus funciones y obligaciones como responsables del fichero almacenado en este sistema[605].

Otro de los aspectos a tener en cuenta es la posibilidad de contratar los servicios de cloud computing con una empresa que no se rija por la LOPD, como puede ser el caso de Dropbox[606], con la que no existe ninguna posibilidad de firmar un contrato de hospedaje de datos. En este supuesto, el cliente -empresa de intermediación- está obligado a adherirse a unas condiciones generales de contratación y, puesto que se produce al mismo tiempo un tratamiento de datos realizado por una empresa ubicada fuera de España, este tratamiento se califica de forma inmediata como una transferencia internacional de datos, para la que habrá que pedir autorización al Director de la AEPD, sobre todo si se trata de un país que no tiene una normativa de protección de datos equiparable a la española.

---

estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente. No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente Capítulo".

[604] Art. 44.3 c) de la LOPD: "*Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave".*

[605] MIRALLES, R: "Cloud computing y protección de datos de carácter personal" *Revista de Derecho, Internet y Política,* núm. 11, 2010. pp.19-21; LEENES, R.:" ¿Quién controla la nube? *IP Revista de Derecho, Internet y Política,* núm. 11, 2010, pp. 5-9; ADSUAR Y.: "Cloud computing vs protección de datos de carácter personal" *Actualidad Jurídica de Aranzadi*, núm. 846,2012.pp.1-4; VV.AA. "La AEPD abre su propia consulta sobre cloudcomputing*" Diario La Ley*, Nº 7784, 2012.

[606] Empresa de almacenaje online que protege la información contenida en ella y permite a las empresas titulares acceder a sus archivos desde cualquier ordenador, teléfono o Tablet.

Una vez más aparece el problema de la falta de información por parte de la empresa de selección a los demandantes de empleo ya que no lo hace sobre cuestiones cómo qué se va a hacer con los datos, sobre todo cuando estas empresas de intermediación deciden crear bases de datos y almacenarlas en los servidores de cloud computing. Las empresas pueden justificar esta actuación sosteniendo que desconocen si van a necesitar estos servicios, y que sólo los contratan a posteriori, una vez que sepan la cantidad de datos que tengan que manejar o las dificultades que planteen la gestión de los mismos.

4. EL TRATAMIENTO DE LOS DATOS ESPECIALMENTE PROTEGIDOS EN LOS PROCESOS DE BÚSQUEDA DE EMPLEO.

4.1. Tratamiento de datos sobre el estado de salud de los demandantes de empleo.

En todo procedimiento de selección de personal el conocimiento del estado de salud, dependiendo del trabajo que vayan a realizar, puede ser un elemento ineludible y en ocasiones determinante para valorar la capacidad profesional de los demandantes de empleo. Por otra parte, también existen ofertas de empleo dirigidas a la colocación de algunos colectivos que presentan alguna discapacidad[607], para las que será requisito indispensable conocer esa condición del candidato al empleo ya que el perfil de la oferta está configurado para estas personas con esa diversidad funcional.

Dicho esto, lo primero que habrá que analizar es para qué tipo de oferta de empleo se hace la selección de personal para realizarla conforme a las características del trabajo a desarrollar en la empresa[608]. En todo caso, y con esta justificación, es posible que haya que averiguar algunas informaciones

[607] Sobre este aspecto véase: GÓMEZ-MILLÁN HERENCIA, M.J.: *Colectivos destinatarios de las políticas selectivas de empleo,* Laborum, 2011, pp. 209-210; GARCÍA MURCIA, J.: "El trabajo de los incapacitados", *Tribuna Social*, núm. 91, 1998, pág. 31; SEMPERE NAVARRO, A.V.: "El trabajo de los minusválidos: Problemas de su regulación", *Tribuna Social*, núm. 91, 1998, pág. 57; TUSET DEL PINO, P.: *La contratación de los trabajadores minusválidos*, Aranzadi, 2000, pp. 55-60.

[608] CARDONA RUBERT, M.B.: Datos sanitarios y relación laboral, Tirant lo Blanch, 1999, pp. 65-70.

relacionadas con el estado de salud del trabajador que, como es sabido, conforman lo que la LOPD ha calificado como datos especialmente protegidos. Siguiendo esta línea de razonamiento, podrían ser legítimas averiguaciones sobre determinadas enfermedades (como el alcoholismo o la toxicomanía) para, por ejemplo, la contratación de un conductor de un medio de transporte público, o sobre la sensibilidad hacia determinadas enfermedades (en el caso de las enfermedades profesionales), mientras sería manifiestamente ilegítima toda averiguación – aún con el consentimiento del trabajador – de la condición de gravidez de una trabajadora postulante a un empleo o de las condiciones de morbilidad de cualquier trabajador para un empleo tradicional para el que esas condiciones carezcan de relevancia[609].

A estos efectos hay que recordar que la LPRL prevé la realización de reconocimientos médicos obligatorios[610] para aquellos supuestos en los que se tenga que verificar el estado de salud del trabajador porque éste pueda constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa; por lo que siguiendo este criterio las pruebas médicas realizadas al demandante de empleo en los procesos de selección de personal también se realizan con la finalidad de no poner en peligro a sus propios compañeros de trabajo o, incluso, a otras sujetos ajenos a la empresa.

Como criterio general, y a los efectos que aquí interesan en cuanto al tratamiento de estos datos que realizan los sujetos encargados de realizar la

[609] BRONSTEIN, A. S.: "La protección de la vida privada en el lugar de trabajo", en *Anales del II Congreso Internacional de Derecho del Trabajo y de la Seguridad Social*, Isla Margarita (Venezuela), 2008, pp. 76-78; ZWERLING, C.: "Current practice and experience in drug and alcohol testing in theworkplace", *Bulletin of Narcotics*, Vol. 45, núm. 2, 1993, pp.155-196.

[610] Art. 22.1 de la LPRL: *"El empresario garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo. Esta vigilancia sólo podrá llevarse a cabo cuando el trabajador preste su consentimiento. De este carácter voluntario sólo se exceptuarán, previo informe de los representantes de los trabajadores, los supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad. En todo caso se deberá optar por la realización de aquellos reconocimientos o pruebas que causen las menores molestias al trabajador y que sean proporcionales al riesgo".*

selección de personal, éste debe realizarse con la máxima cautela y sólo con el objetivo de comprobar la adecuación del trabajador al puesto de trabajo demandado[611]. Se puede afirmar que la entidad que realiza la selección de personal está facultada para efectuarlos, o más bien, para encomendar esta tarea a una empresa encargada de esta actividad, siempre que sea necesario por las especiales condiciones de la tarea que vaya a realizar[612]. En estos casos, el responsable de ese fichero de datos de salud y de comunicar al seleccionador de personal tan sólo la aptitud o no del futuro trabajador para desempeñar el trabajo demandado, es la empresa encargada de realizar los

[611] Por este motivo, el TSJ de Madrid en su Sentencia de 16 de junio de 2015 (AS 2015\1304) ha estimado que el padecimiento de una concreta enfermedad por el aspirante al puesto de trabajo no es motivo para que quede excluido del proceso de selección, ya que el procesamiento de ese dato tiene como objetivo valorar la capacidad del trabajador, el cual es realmente apto para efectuar la tarea que se le pretende encomendar: *"La principal norma de referencia en la materia es la Ley 31/1995, de 8 de noviembre (RCL 1995, 3053) , de Prevención de Riesgos Laborales (LPRL), en particular su art. 22 . Todas las partes la invocan en estos autos, lo mismo que los órganos judiciales. Pues bien, poniendo el acento en los perfiles del caso, deben destacarse en aquélla los siguientes caracteres y principios: la determinación de una vigilancia periódica -y como regla general consentida- del estado de salud de los trabajadores en función de los riesgos inherentes a su actividad laboral; la voluntariedad del sometimiento a los reconocimientos médicos; la existencia de situaciones tasadas en las que resulta imprescindible la realización de las exploraciones médicas, limitándose así, excepcionalmente en esos casos, la libre determinación del sujeto; el principio de la indispensabilidad de las pruebas y de su proporcionalidad al riesgo ; el necesario respeto del derecho a la intimidad, a la dignidad de la persona y a la confidencialidad de la información relacionada con su estado de salud; el derecho del trabajador a conocer los resultados; la prohibición de utilización de los datos relativos a la vigilancia de la salud con fines discriminatorios o en perjuicio del trabajador ; la prohibición de comunicación de la información resultante, salvo que exista consentimiento expreso del trabajador, y la posibilidad de transmitir al empresario y a las personas u órganos con responsabilidades en materia de prevención únicamente las conclusiones que se deriven de las exploraciones, y con el exclusivo objeto de que puedan desarrollar sus funciones en materia preventiva".*

[612] Art. 243 del RD 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social (BOE núm. 261 de 31 de octubre de 2015):: *"1. Todas las empresas que hayan de cubrir puestos de trabajo con riesgo de enfermedades profesionales están obligadas a practicar un reconocimiento médico previo a la admisión de los trabajadores que hayan de ocupar aquéllos y a realizar los reconocimientos periódicos que para cada tipo de enfermedad se establezcan en las normas que, al efecto, dictará el Ministerio de Trabajo y Seguridad Social. 2. Los reconocimientos serán a cargo de la empresa y tendrán el carácter de obligatorios para el trabajador, a quien abonará aquélla, si a ello hubiera lugar, los gastos de desplazamiento y la totalidad del salario que por tal causa pueda dejar de percibir. 3. Las indicadas empresas no podrán contratar trabajadores que en el reconocimiento médico no hayan sido calificados como aptos para desempeñar los puestos de trabajo de las mismas de que se trate. Igual prohibición se establece respecto a la continuación del trabajador en su puesto de trabajo cuando no se mantenga la declaración de aptitud en los reconocimientos sucesivos. 4. Las disposiciones de aplicación y desarrollo determinarán los casos excepcionales en los que, por exigencias de hecho de la contratación laboral, se pueda conceder un plazo para efectuar los reconocimientos inmediatamente después de la iniciación del trabajo".*

citados exámenes médicos[613]. Por lo que el seleccionador no tiene derecho a conocer todo el contenido del reconocimiento realizado, sino sólo las conclusiones que guarden relación con la capacidad del trabajador y la mejora de las medidas de protección[614]. En estos casos no habría tratamiento de datos de salud porque realmente sólo se conoce la capacidad para desempeñar es tarea determinada.

Cosa distinta es el tratamiento de datos relacionados con la salud que realiza la empresa que realiza el examen médico para certificar la aptitud para ese concreto puesto de trabajo. Obviamente, el almacenamiento de datos que efectúan los sanitarios de la citada empresa constituye un tratamiento de datos relacionados con la salud de los trabajadores, el cual debe cumplir con los principios de la LOPD y con las exigencias de confidencialidad de esa información previstas para el personal médico[615].

Sin embargo, cuando lo que se pretende es hacer una selección de personal para una oferta de empleo específica en la que haya que acreditar algún grado de discapacidad[616] del demandante de empleo, concebido como requisito indispensable para poder participar en el proceso de selección en

[613] Sobre los reconocimientos médicos de los trabajadores vid., apartado 3.1 del tercer Capítulo.

[614] FERNÁNDEZ DOMÍNGUEZ, J.J.: "Test de alcohol y drogas en el trabajo: la selección de la prueba más respetuosa con los derechos fundamentales del trabajador" en VV.AA. *Los derecho fundamentales inespecíficos en la relación laboral y en materia de protección social*, Cinca, 2014, disponible en CD; TALENS VISCONTI, E.: "La vigilancia de la salud del trabajador y el respeto a su intimidad en el supuesto consumo de drogas", *Revista Española de Drogodependencias*, núm. 2, 2013, pp. 186-189; APDCM: " Tratamiento de datos de salud con la finalidad de promover la adaptación de su puesto de trabajo", *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, núm. 40, 2009, pp. 20-25; DESDENTADO BONETE, A. Y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y…,* op. cit., pág.111.

[615] Sobre la problemática del tratamiento de datos de salud por los distintos sujetos encargados de realizar los reconocimientos médicos de los trabajadores se va a incidir en el apartado 3.1 del Capítulo III.

[616] Obviamente, aunque la discapacidad no es una enfermedad está intrínsecamente relacionada con el estado de salud de la persona y, por tanto, siguiendo lo establecido en el art. 5 g) del RDLOPD: *"Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética",* estos datos son considerados especialmente protegidos. Así lo ha entendido también la jurisprudencia en la Sentencia de la Audiencia Nacional de 27 de abril de 2005 (JUR 2006\196759) cuando establece que evidentemente el porcentaje de discapacidad de un individuo es un dato relativo a la salud.

razón de los aspectos descriptivos del empleo, la cuestión es diferente pues será el propio candidato el que notifique esta circunstancia al sujeto que realiza la tarea de elección del trabajador[617].

Por este motivo, se entiende que en este caso[618] sí se está realizando un tratamiento de datos[619], ya que el seleccionador conoce esa información directamente del candidato de empleo, facilitándola con la intención de participar en ese concreto proceso de selección. La empresa de intermediación la almacena en sus ficheros de datos sobre los candidatos al empleo, pudiendo, incluso, comunicar esta circunstancia al empresario que demanda el trabajo.

En este tratamiento de datos, el sujeto que realiza la selección debe certificar que ese procesamiento es imprescindible para acreditar el cumplimiento de los requisitos planteados en la oferta de trabajo, respetando el principio de calidad de los datos y no usando esa información para otras finalidades incompatibles. Para lograr este objetivo estas informaciones tratadas deben ser proporcionales y certeras, es decir, que no puedan conducir a duda o error, ya que si así fuera podría afectar a los candidatos de empleo sobre todo si finalmente no son contratados alegando que no cumplen con los requisitos solicitados por la empresa relacionados con la tenencia de una concreta discapacidad.

---

[617] Algunos autores han definido la discapacidad laboral como una deficiencia de naturaleza física, psíquica, sensorial o intelectual que impide participar a la persona, bajo criterio de igualdad y efectividad en todos los aspectos de la comunidad. Consecuentemente, no se trata tanto de eliminar las deficiencias que provoca la discapacidad, como de evitar que la misma impida a la persona que la padece acceder bajo unos parámetros de igualdad y efectividad a los diversos aspectos que componen la vida en comunidad, garantizando la igualdad de oportunidades". Vid., GARCÍA QUIÑONES, J.C.: "El concepto jurídico laboral de discapacitado" en VALDÉS DAL-RE, F. Y LAHERA FORTEZA, J.: *Relaciones laborales de las personas con discapacidad*, Ed. Biblioteca Nueva, 2005, pág. 84; GARRIDO PÉREZ, E.: "El tratamiento comunitario de la discapacidad", *Revista Temas Laborales* , núm. 59, 2001, pág. 173

[618] Como se ha comentado cuando tan sólo se comunica al intermediador la aptitud del demandante de empleo para realizar esa concreta tarea para la cual se ha realizado el reconocimiento médico, debido a las especiales características del puesto de trabajo demandado, no se está realizando un tratamiento de datos relacionados con la salud de éste, ya que no se traslada esa información y se queda en los registros de la empresa que realiza los citados reconocimientos.

[619] DE VICENTE PACHÉS, F.: "Protección de datos personales y agentes…", op. cit., pp. 17-19; SÁNCHEZ CARAZO, C.: "La protección de datos personales de las personas vulnerables" *Anuario de la Facultad de Derecho*, núm. 2, 2009, pp. 214-226.

Para realizar de forma correcta este procesamiento ha de mediar el consentimiento expreso del candidato al empleo, que se supone que se otorga pues él mismo es el que aporta esa información médica al seleccionador. De forma particular, también en el marco de la selección de personal, las excepciones al consentimiento para tratar datos relativos a la salud de los candidatos al empleo no operaría en ningún supuesto; salvo que alguna norma de rango legal así lo estableciera o se diera algún caso en el que el procesamiento del dato fuera necesario para proteger un interés vital del afectado[620]. Lo que, en estos supuestos de selección de personal, no tiene por qué materializarse pues lo único que se pretende es realizar un concreto tratamiento del dato a fin de corroborar que el candidato cumple con los requisitos exigidos en la oferta de empleo. De cualquier modo, es obvio que el registro de estos datos sobre la discapacidad de los futuros trabajadores debe cumplir las garantías previstas en la LOPD y, al tratarse de datos especialmente protegidos, el responsable del fichero, persona o entidad que realiza la selección tendrá que implantar medidas de seguridad de nivel alto, conforme a lo establecido en el art. 81.3 del RDLOPD.

Puede ocurrir que, en la selección de personal, este procesamiento de datos, se derive a otra empresa o fundación vinculada o dependiente, por ejemplo, de una ETT[621], siendo éstas las que ofrecen directamente el empleo y recepcionan los CVs a través de su web o por medio de su entrega física en alguna de sus sedes. A pesar de esto, existe la posibilidad de que la gestión de esta selección de personal la realice, finalmente, una fundación perteneciente a la propia ETT. En estos casos se produce por parte de la ETT una comunicación de esta información sobre la discapacidad del futuro trabajador a la fundación, aunque su publicidad y el almacenamiento de solicitudes sea una labor realizada en primera instancia por la ETT[622].

[620] Art. 7.3 y 6 de la LOPD.
[621] Algunos ejemplos de fundaciones que gestionan directamente ofertas de empleo para personas con capacidades especiales: Fundación Adecco (http://www.fundacion adecco.es/Home/Home.aspx), Fundación Manpower (http://www.fundacionmanpower.org/), Fundación Randstad Empleo (http://www.randstad.es/fundacion).
[622] APDCM: "Tratamiento de datos de salud para adaptaciones curriculares" *Revista de la Agencia de Protección de datos de la Comunidad de Madrid*, núm. 34, 2008, pp. 1-3.

Para estas comunicaciones o cesiones de datos sobre el estado de salud del futuro trabajador será preciso su consentimiento expreso, porque no queda del todo claro si podría caber alguna de las excepciones tasadas en la LOPD. A pesar de ello, si se hiciera una interpretación flexible del art. 11.2 c) de la LOPD[623], se podría prescindir del citado consentimiento, siempre que esa cesión tuviera como pretensión conseguir colaborar en las tareas de colocación del trabajador y para ello fuera necesario comunicar ese dato, en este caso, a una fundación encargada de gestionar determinadas ofertas de empleo para las cuales se tiene que conocer datos sobre discapacidad o del candidato, con la particularidad que esta fundación mantiene una relación jurídica con la ETT.

En las empresas de intermediación pública[624] también se hace preciso, algunas veces, el conocimiento de datos relativos a alguna discapacidad que tenga el candidato al empleo, ya que para estas personas se prevé un acompañamiento reforzado en la búsqueda de empleo y se ofrece un servicio personalizado para la mejora de sus niveles de empleabilidad, mediante el diseño de itinerarios de inserción virtuales e individualizados para cada caso concreto. Estos itinerarios de inserción, creados en el marco de actividades del SEPE[625], usan datos especialmente sensibles de los ciudadanos y, por ello, tendrán que respetar las exigencias establecidas, no sólo en la normativa sobre protección de datos, sino también las mencionadas en la Orden de 26 de septiembre de 2014, relacionadas con el tratamiento de datos y el uso de las bases de datos constituidas para poder hacer un seguimiento de estos itinerarios de inserción[626]. Aunque, en lo que a la cesión se refiere, se podría

---

[623] Art. 11.2 c) de la LOPD*: "Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique".*

[624] Sobre los distintos usos de los datos de discapacidad como consecuencia de los distintos mecanismos existentes en la intermediación pública para colocar a estos candidatos vid., LAHERA FORTEZA, J.: "Acceso al mercado de trabajo y contratación de los discapacitados" en en VALDÉS DAL-RE, F. Y LAHERA FORTEZA, J.: *Relaciones laborales de las personas…,* op. cit*.,* pp. 99-113.

[625] Véase, Orden de 26 de septiembre de 2014, por la que se desarrollan los programas de orientación profesional, itinerarios de inserción y acompañamiento a la inserción regulados por el Decreto 85/2003, de 1 de abril (BOE núm. 193 de 2 de octubre de 2014).

[626] Art. 14.5 Orden de 26 de septiembre de 2014: *"Las actuaciones que lleven aparejadas cesión de datos de carácter personal se ajustarán a lo dispuesto en la Ley Orgánica 15/1999,*

producir la excepción al consentimiento si esa comunicación tiene lugar entre administraciones públicas, como podría ser el caso en la intermediación pública, y sólo se hiciera para cumplir con fines estadísticos.

También las agencias de recolocación pueden hacer un uso de los datos relativos a la salud de los solicitantes de sus servicios, por ejemplo, se realizan tratamientos de datos al almacenar en sus ficheros datos psicológicos de los trabajadores que se someten a su programa de recolocación, relacionados, muchos de ellos, con episodios de ansiedad seguramente causados por la situaciones vividas en torno al despido.

4.2. Tratamientos de datos ideológicos en los procesos de selección de personal.

Como regla general, los datos sobre ideología no pueden ser indagados o tenidos en cuenta en un proceso de selección[627]. No obstante, en el caso de la selección de personal para algunas empresas calificadas como ideológicas o de tendencia[628], se permite que se hagan indagaciones sobre la ideología de los candidatos al empleo, aunque siempre conforme a las reglas generalmente aceptadas, haya que diferenciar entre los trabajadores que realizan actividades relacionadas con la ideología de la empresa, colaborando en su creación y

de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normas de aplicación". Art. 18 de la Orden de 26 de septiembre de 2014: *"La Agencia Servicio Andaluz de Empleo realizará el seguimiento y la evaluación del Programa de Orientación Profesional al objeto de conocer y mejorar el desarrollo de las acciones ejecutadas. Para ello, valorará los resultados de las acciones en términos de inserción laboral, calidad de los servicios y satisfacción de las personas usuarias obtenidos a través de encuestas de resultados, cruces de bases de datos u otras acciones que se consideren de aplicación, verificará la actividad desarrollada y aplicará programas de evaluación del desempeño profesional".*

[627] Existe en nuestro texto constitucional (art. 16.2) una prohibición genérica de indagar respecto a estas circunstancias, "nadie podrá ser obligado a declarar sobre su ideología, religión o creencias", prohibición que tiene su traslación al ámbito laboral (arts. 4.2.c) y 17.1 del ET), en cuanto a las posibles consecuencias discriminatorios que puedan derivarse del uso que de tales informaciones pudiera hacer el empleador o agente mediador en la colocación.

[628] Una empresa de tendencia o ideológica es aquella que se intenta diferenciar de las demás manifestando abiertamente su afinidad con una concreta ideología, normalmente política o religiosa, con el fin de captar a los clientes potenciales que comparten la misma opinión, en ARESE, C.: "Empresas ideológicas o de tendencia" en VV.AA.: *Diccionario internacional de derecho del trabajo y de la seguridad social*, Tirant lo Blanch, 2014, pp. 851-853.

difusión, mientras que otros trabajan en tareas técnicas o funcionales para los cuales no es necesario tener el citado perfil ideológico[629].

Por este motivo, estas opiniones ideológicas no tendrán sentido si la tarea que va a desarrollar el trabajador, incluso en la propia empresa de tendencia, no está relacionada con el ideario que la misma pretende transmitir al tratarse de unja tarea de las calificadas como neutras. Pero si la actividad que va a realizar está vinculada con un supuesto pensamiento ideológico, la averiguación de esta información puede ser clave, por lo que estas indagaciones se consideran legítimas pudiéndose entender necesarias para valorar su aptitud o idoneidad, sobre todo para la difusión de la ideología de la que es expresión institucional la organización a la que va a pertenecer[630].

Así lo ha reconocido la jurisprudencia en la Sentencia del Tribunal Constitucional 77/1985 de 27 de junio[631]: "*No cabe duda alguna de que la facultad de seleccionar al profesorado que se estime más idóneo forma parte del derecho a crear y dirigir centros docentes que nuestra Constitución consagra. Tampoco es dudoso, sin embargo, que al garantizar el derecho de los profesores, los padres y en su caso, los alumnos, a intervenir en el control y gestión de todos los centros sostenidos por la Administración con fondos públicos en los términos que la Ley establezca, la C.E. (art. 27.7) habilita al legislador para condicionar o restringir aquella facultad en los términos que considere más oportunos para dar contenido concreto a este derecho de los restantes miembros de la comunidad escolar".*

[629] BLAT GIMENO, F.: *Relaciones laborales y empresas ideológicas*, Ministerio de Trabajo y Seguridad Social, 1986, pp.102-105; MOTILLA DE LA CALLE, A.: "El derecho a discriminar en las relaciones laborales excepciones a la prohibición general de discriminar por motivos ideológicos o religiosos en Europa", *Revista Española de Derecho del Trabajo y de la Seguridad Social,* núm. 158, 2013, pp. 108-110.

[630] En este sentido RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, M.: "No discriminación en las relaciones laborales" en *Comentarios a las Leyes Laborales. El Estatuto de los trabajadores, Tomo IV*, 1983, pág. 379-380; APARICIO TOVAR, J.: "Relación de trabajo y libertad de pensamiento en las empresas ideológicas", en *Lecciones de Derecho del Trabajo en homenaje a los profesores Bayón Chacón y Del Peso Calvo*, Universidad Complutense de Madrid, 1980, pp. 296; MORENO BOTELLA, G.: *La libertad de conciencia del trabajador en las empresas ideológicas confesionales,* Fundación Universitaria Española, 2003, pp.254-257.

[631] BOE núm.170 de 17 de julio de 1985.

Por tanto, a la hora de realizar una selección de personal para este tipo de empresas, habrá que distinguir, en primer lugar, qué tarea va a desempeñar el candidato en la empresa y, en segundo lugar, efectuar una selección de personal más específica que respete la ideología de la empresa cuando ese respeto o convicción sea necesario para la ejecución de la actividad[632]. Una vez concretada la necesidad de conocer esa información del futuro trabajador, es preciso atender a lo establecido en la normativa sobre protección de datos relativa al tratamiento de datos sobre ideología. Así, lo normal es que la información venga directamente del propio candidato a partir de las preguntas que le haga el seleccionador en una entrevista de trabajo. Ciertamente, esta forma de proporcionar los datos ideológicos no presenta, en principio, ningún problema ya que con estas averiguaciones no se está produciendo ningún tratamiento de datos sino su mera consulta[633].

Pero no cabe duda que el entrevistador, en un proceso amplio de selección de candidatos, normalmente almacenará la información obtenida, y es en este punto dónde se puede empezar a hablar de tratamiento de datos. Sin embargo, aunque la LOPD prohíbe la creación de ficheros con datos ideológicos[634], éstos podrán constituirse si el titular de esa información consiente expresamente y por escrito la inclusión de esa información sobre su ideología en un fichero. Por lo que, si se produce ese tratamiento a través del registro de esos datos, hay que dejar claro que, para cumplir con el principio de calidad en el procesamiento de datos, esta información sensible del futuro

[632] GOÑI SEÍN, J.L.: *El respeto a la esfera…,* op. cit., pp. 70-74; DE VAL TENA, A.L.: *"*Las empresas de tendencia ante el Derecho del Trabajo: libertad ideológica y contrato de trabajo", *Proyecto social: relaciones laborales*, núm. 2, 1994, pp. 177-198; SELMA PENALVA, A; *"*La transcendencia práctica de la "vinculación ideológica" en las empresas de tendencia en el ámbito de las relaciones de trabajo" *Anales de Derecho*, núm. 26, 2008, pp. 300-302; SEMPERE NAVARRO, A.V.: "La existencia de Dios y los trabajadores"*, Actualidad Jurídica Aranzadi,* núm. 77, 2009; RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, M.: "Libertad ideológica, contrato de trabajo y objeción de conciencia", *Revista Relaciones Laborales*, núm. 2, 2003, pp. 55-68; VALDÉS DAL-RE, F.: "Libertad ideológica y contrato de trabajo: una aproximación de Derecho comparado", *Revista Relaciones Laborales*, núm. 2, 2004, pp.17-26.

[633] QUÍLEZ AGREDA, E.: "Datos especialmente protegidos: tratamiento de los ficheros de afiliados de los partidos políticos en los procesos electorales internos: Título II. Principios de la Protección de Datos. artículo 7.2" en TRONCOSO REIGADA, A.: *Comentario a la Ley Orgánica de…,* op. cit., pp. 631-647; DE VICENTE PACHÉS, F.: "Protección de datos personales y agentes…", op. cit., pp. 15-16.

[634] Art. 7.4 de la LOPD: *"Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual".*

trabajador tan sólo se va a utilizar para corroborar su idoneidad a la hora de realizar las tareas ideológicas que la empresa le pueda encomendar. Es decir, no se permite cualquier otro tipo de tratamiento que no atienda a estas características, como así lo ha señalado la jurisprudencia en la Sentencia del Tribunal Superior de Justicia de Islas Canarias de 17 de julio de 2007[635] que establece que la forma más sencilla de proceder ante la colisión del derecho del trabajador a proteger su información personal con el del empresario a organizar libremente su empresa, es atender al principio de calidad de los datos, por lo que habrá que determinar si el requerimiento de esos datos puede ser excesivo o desproporcionado para el objetivo deseado[636].

---

[635] AS 2007\2185: *"El derecho a la libertad religiosa y el principio de neutralidad religiosa del Estado implican que la impartición de la enseñanza religiosa asumida por el Estado en el marco de su deber de cooperación con las confesiones religiosas se realice por las personas que las confesiones consideren cualificadas para ello y con el contenido dogmático por ellas decidido. Sin embargo, por más que haya de respetarse la libertad de criterio de las confesiones a la hora de establecer los contenidos de las enseñanzas religiosas y los criterios con arreglo a los cuales determinen la concurrencia de la cualificación necesaria para la contratación de una persona como profesor de su doctrina, tal libertad no es en modo alguno absoluta, como tampoco lo con los derechos reconocidos en el art. 16 CE ni en ningún otro precepto de la Constitución, pues en todo caso han de operar la exigencias inexcusables de indemnidad del orden constitucional de valores y principios cifrado en la cláusula del orden público constitucional" (Fj. 7)-"Los órganos jurisdiccionales (son) los que deben ponderar los diversos derechos fundamentales en juego" y en el ejercicio de este control "habrán de encontrar criterios practicables que permitan conciliar en el caso concreto las exigencias de la libertad religiosa* (individual y colectiva) *y el principio de neutralidad religiosa del Estado con la protección jurisdiccional de los derechos fundamentales y laborales de los profesores".* En el mismo sentido, vid., Sentencia núm. 213/2011 de 3 de mayo del Juzgado de lo Social de Almería(AS 2011\1151) sobre la no renovación del contrato a profesor de religión por motivos ajenos a la actividad; *La parte actora pretendía con su demanda que su no nombramiento para impartir clases de Religión y Moral Católicas en el curso escolar 2001/02 se considerara como un despido y que el mismo fuera declarado nulo pues se había realizado con vulneración de sus derechos fundamentales, ya que la no propuesta por parte del Obispado de Almería al Ministerio de Educación y Cultura y Deporte (hoy Ministerio de Educación) había sido debido única y exclusivamente al hecho de haber contraído matrimonio civil, lo cual supuso un trato discriminatorio pues vulneró el principio de igualdad consagrado en el art. 14 de nuestra Constitución así como una violación del derecho fundamental a la intimidad personal y familiar recogido igualmente en el art. 18 de la Constitución Española. … Por lo tanto es evidente que si la única causa para la no renovación de la demandante como profesora de religión y moral católica era que la misma había contraído matrimonio civil con una persona divorciada, es decir un motivo totalmente ajeno a la actividad docente desempeñada, está claro que dicha decisión supone no solo una vulneración de su derecho fundamental a la libertad ideológica consagrado en el art 16 de la Constitución Española conectado con el derecho a contraer a matrimonio en la forma legalmente establecida (art 32 CE), sino un también trato discriminatorio por razón de matrimonio que viola el derecho fundamental a la igualdad recogido en el art 14 de la CE y un atentado al derecho fundamental a la intimidad personal y familiar de la trabajadora".*

[636] DE VICENTE PACHÉS, F.: *El derecho del trabajador al*…, op. cit., pp. 154-156; VAL TENA, A.L.: "Las empresas de tendencia ante…", op. cit., pp. 188-190; CALVO GALLEGO, F.J: *Contrato de trabajo y Libertad ideológica. Derechos fundamentales y organizaciones de tendencia* CES, Colección Estudios 1995. pp. 188-192; GÓMEZ-MILLÁN HERENCIA, M.J: "Extinción del contrato de trabajo. El despido por razones ideológicas en la Administración Pública*", Temas Laborales* núm. 108, 2001, pp. 269-270.

Además de comprobar que estas informaciones se registran con esa única finalidad, es preciso que el seleccionador informe al titular del dato –candidato al empleo- sobre el uso y destino que se le va a dar a ese dato. Asimismo, para cumplir con el principio de información hay que acudir a lo establecido en el art. 5 de la LOPD[637]y, además, advertir sobre el derecho que tiene ese candidato a que sus datos no sean tratados. Sobre la negativa a este tratamiento de datos se puede decir que, en el caso de la selección de personal para empresas de tendencia, puede que sea imprescindible el conocimiento de ese dato ideológico si, como se ha dicho, es criterio ineludible para acreditar su capacidad profesional. No obstante, el demandante de empleo puede conocer la necesidad de aportar esa información si previamente en la oferta de empleo vienen preestablecidas las características del empleo y, entre ellas, aparezca la acreditación de ese perfil ideológico. Este hecho podría considerarse como una advertencia realizada a todos los interesados en la oferta, ya que a partir de ella pueden saber qué es lo que se requiere y que datos van a ser tratados por el intermediador.

En referencia al consentimiento que tiene que prestar el demandante de empleo para que esos datos ideológicos sean tratados, como se conoce, la normativa sobre protección de datos establece que éste tendrá que ser expreso y, además, constar por escrito. Se entiende que este consentimiento no se puede exceptuar pues la norma no establece las particularidades del señalado art. 6.2 LOPD cuando se traten datos especialmente protegidos, independientemente de que estas informaciones sean tratadas para mantener o permitir el cumplimiento de una relación precontractual o contractual.

[637] Art. 5.1 de la LOPD: *"1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento".*

En el marco de un proceso de selección, lógicamente, los datos sobre ideología del candidato al empleo pueden ser trasladados a la empresa que demanda el trabajo, pero con la particularidad de que, además de ser informado el titular del dato de que se va a producir esa cesión, se tiene que pedir su consentimiento expreso y por escrito si en esa empresa se fueran a registrar esos datos en un fichero, cuyo responsable será ahora la empresa en la que se va a incorporar el trabajador. Aunque sobre este punto, lo normal es que la empresa también valore la idoneidad del candidato ya que este criterio sobre la concreta ideología que debe tener el demandante de empleo es algo más subjetivo que cualquier otra información necesaria para realizar la selección de personal, por lo que será la empresa la que, en última instancia, decida si reúne las características deseadas para desempeñar la tarea ideológica que se le encomiende.

5. TRANSFERENCIA INTERNACIONAL DE DATOS COMO INSTRUMENTO DE INTERMEDIACIÓN LABORAL.

Hoy día es necesario que la información de las ofertas de empleo pueda fluir entre las distintas sedes que ofrezcan un empleo, ya sean nacionales o transnacionales. A estos efectos, hay que delimitar qué se entiende por transferencia internacional de datos para lo cual es preciso acudir a lo señalado en el art. 33 de la LOPD[638], donde se establece que no podrán transferirse datos, de forma temporal ni definitiva que hayan sido objeto de tratamiento o recogidos con ese objetivo, a países que no otorguen un nivel de protección equiparable al establecido por la LOPD. Pero si, a pesar de esta prohibición, se quiere realizar la transferencia, ésta tendrá que ser autorizada previamente por

[638] Art. 33 de la LOPD: "*1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".*

la AEPD que evaluará el nivel de protección que establece el país de destino de los datos[639].

Por su parte, la Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección, relativa a las normas por las que se rigen los movimientos internacionales de datos[640], hace referencia también al concepto de transferencia internacional como "*toda transmisión de los mismos fuera del territorio español. En particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero"*. También en el art. 5.1 s) del RD 1720/2007[641] se especifica que se considerará transferencia internacional de datos la que se realiza a países externos al Espacio Económico Europeo, por lo que matiza un poco más lo establecido en la LOPD ya que en ésta no se detalla el destino exacto de esta actuación.

Ciertamente, una persona que se encuentra en situación de desempleo y pide colaboración a las empresas de intermediación para que le ayuden a encontrar un empleo, estará seguramente dispuesta a encontrar un trabajo y desarrollarlo en otros países además de en España; por lo que, en un principio, estará de acuerdo con la cesión de sus datos de carácter personal a terceros países para así ampliar sus posibilidades de obtener un empleo acorde con sus características profesionales. Pero esta sencilla operación implica, sin embargo, una importante problemática en lo que a la protección de datos de carácter personal se refiere, en la medida en que dichas

---

[639] Respecto a las circunstancias para constatar el nivel adecuado de protección, el art. 33.2 de la LOPD se basa literalmente en lo establecido en el art. 25.2 de la Directiva 95/46/CE; *"El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidasde seguridad en vigor en dichos países".*

[640] Fuente: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/. [Consulta 26/12/2014].

[641] Art. 5.1 s) del RDLOPD: *"Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español."*

transferencias de datos tienen que respetar las exigencias establecidas en la normativa española sobre protección de datos.

En primer lugar, para poder certificar el cumplimiento de estas obligaciones, a la hora de realizar una transferencia internacional de datos, es necesario identificar a los sujetos que intervienen los cuales vienen definidos en el art. 5.1 a), h), i), j) q) y ñ) del RDLOPD[642]. En lo que a los procesos de búsqueda de empleo se refiere, los sujetos intervinientes en una operación de intermediación laboral con cariz internacional son: el afectado o titular de los datos que será el ciudadano que pretenda buscar un empleo; la empresa de intermediación que tiene en su poder esa información y que realiza su tratamiento con el consentimiento previo de su titular, convirtiéndose en el exportador o responsable del fichero de datos; y, por otro lado, el importador de los mismos que será la empresa situada en un tercer país que recibe esos datos.

En segundo lugar, con la intención de la transferencia de datos sea acorde con la LOPD, el sujeto que emite los datos tiene que cumplir una serie de requisitos[643], que podrán excepcionarse, si el Estado receptor de esos datos de carácter personal ofrece un nivel adecuado de protección, o si concurre

[642] Art. 5.1 del RDLOPD: "*a) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento. h) Destinatario o cesionario: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. i) Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. j) Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero. q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. ñ) Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero".*

[643] Art. 66.1 del RDLOPD: "*Para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del presente reglamento. La autorización se otorgará conforme al procedimiento establecido en la sección primera del Capítulo V del título IX de este reglamento".*

alguna de las causas de excepción previstas en el art. 34 de la LOPD apartados de la a) a la j)[644]. En primer lugar y para concretar qué países gozan de un nivel adecuado de protección hay que atender a lo establecido en distintas decisiones de la Comisión Europea, siendo los países que gozan de este nivel: Suiza y las entidades estadounidenses adheridas a los principios de «Puerto Seguro», Islandia, Liechtenstein, Noruega, Argentina, Guernsey, Isla de Man, Canadá, Jersey, Islas Feroe, Andorra e Israel así como los Estados miembros de la Unión Europea. Con la consecuencia de que las transferencia de datos que se hagan a estos países no precisarán la autorización de la AEPD, tal y como establece el art. 68 del RDLOPD[645].

En cambio, si la transferencia internacional de datos tiene por destino un país para el que no se ha reconocido un nivel de protección equiparable al de la normativa española sobre protección de datos y no se dan las excepciones del citado art. 34 de la LOPD, además de observarse lo dispuesto en esta norma, es preciso obtener la autorización del Director de la AEPD, de acuerdo con lo establecido en el art. 33.1 de la LOPD. Una autorización que sólo se otorga cuando el responsable del tratamiento ofrece garantías suficientes

[644] Art. 34 de la LOPD: "*Lo dispuesto en el artículo anterior no será de aplicación: a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España. b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional. c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios. d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica. e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista. f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado. g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero .h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias. i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial. j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo. k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado".*

[645] Art. 68 del RDLOPD: *"No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección".*

respecto de: la protección de la vida privada, de los derechos y libertades fundamentales, de la protección de datos de las personas, así como respecto del ejercicio de todos estos derechos.

Estas garantías deben quedar reflejadas en la redacción de determinadas cláusulas contractuales[646] entre exportador e importador de datos redactadas de acuerdo con lo establecido en el art. 70.2 del RDLOPD[647] que dispone que la autorización se dará cuando el exportador presente un contrato escrito entre él y el que recibe los datos que acredite de forma suficiente la protección de los datos de carácter personal de aquellas personas afectadas por la transferencia[648]. Pese a ello, existen una serie de supuestos en los que se podrá denegar la autorización de la AEPD para realizar el movimiento internacional de datos, siempre que: no se cumplan las cláusulas contractuales fijadas en el acuerdo entre exportador e importador; que no se pueda realizar lo acordado en el contrato debido a que el país de destino impida su cumplimiento; que existan indicios razonables de que las garantías establecidas en el contrato no están siendo cumplidas por el importador o que los mecanismos de aplicación del contrato no sean efectivos; y, por último, que la transferencia pudiera suponer una situación de riesgo para los afectados[649].

---

[646] Sobre el contenido de estas cláusulas contractuales vid., *Decisiones de la Comisión Europea 2004/915/CE, de 27 de diciembre de 2004* (Anexo II en el que se describen los siguientes apartados: definiciones; obligaciones de importador y exportador de datos; responsabilidades de terceros; legislación aplicable; resolución y variación de las cláusulas; y contenido de la transferencia internacional de datos)*; Decisión de la Comisión Europea 2002/16/CE, de 27 de diciembre de 2001* (Anexo cuyo contenido es el siguiente: definiciones, detalle de la transferencia, cláusula de tercero beneficiario; obligaciones de exportador e importador de datos; responsabilidades; legislación aplicable; mediación y jurisdicción; cooperación con autoridades de control; obligaciones una vez terminada la prestación de servicios al encargado del tratamiento; y variación del contrato).

[647] Art. 70.2 del RDLOPD: "*La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos. A tal efecto, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, 2002/16/CE, de 27 de diciembre de 2001, y 2004/915/CE, de 27 de diciembre de 2004 o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE".*

[648] SAN JUAN GARCÍA, P.: "Nuevas reglas de juego en la protección de datos", *Revista Lex Nova*, núm. 52, 2008, pp. 6-7.

[649] Vid., art. 70.3 del RDLOPD.

Los contratos citados, tal y como establece el RDLOPD, deben respetar las rigurosas exigencias establecidas por distintas decisiones de la Comisión Europea[650]. Parece que la norma ha querido salvaguardar la protección de esos datos recurriendo a la voluntad conjunta del responsable del fichero y de la entidad que va a recibirlos para, de esta forma, poder verificar si la destinataria de la información puede asegurar ese nivel de protección y si la normativa de su país le permite cumplir con las características del contrato[651].

Ciertamente, la única forma de comprobar el grado de cumplimiento de las exigencias de la LOPD en el movimiento internacional de datos propiciado por las empresas o medios de intermediación es examinar su política de privacidad y, una vez hecho esto, se puede decir que, por ejemplo, en el caso de las empresas de trabajo temporal se observa cómo no se suele hacer referencia a la transferencia internacional de datos; una carencia extraña ya que la finalidad de estas empresas es la colocación e incluso la contratación de los demandantes de empleo y con la transmisión de datos a empresas extranjeras se puede alcanzar un mayor éxito en su tarea[652].

En otros casos, la propia web de la ETT hace referencia en una sección específica para ello a la posibilidad de que el candidato de empleo se inscriba en cualquier oferta que se vaya a desarrollar fuera de España. Por este motivo, aunque este aspecto no se contemple en la política de privacidad de la web, obviamente, el envío de sus datos a esas ofertas de empleo internacionales constituye una transferencia internacional de datos. Además, de este servicio web, las propias agencias tienen sucursales en el extranjero que ponen en

---

[650] Decisiones de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, 2002/16/CE, de 27 de diciembre de 2001, y 2004/915/CE, de 27 de diciembre de 2004 o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.

[651] RUBÍ NAVARRETE, J.*: "Transferencia internacional de datos" en VV.AA.: XVII Encuentros de Derecho e Informática, Universidad Pontificia Comillas, 2003, pp.15-22; BARCELÓ, R.: "Transferencia internacional de datos personales" en VV.AA.: Protección de datos comentarios a la LOPD y su reglamento de desarrollo, Tirant lo Blanch, 2009, pp. 141-166; ABERASTURI GORRIÑO, U.: "Movimiento Internacional de Datos. Especial referencia a las transferencia internacional de datos sanitarios" Revista de Administración Pública, núm. 186, 2011, pp. 88, 345-350.*

[652] Empresas de trabajo temporal que no hacen alusión en su política de privacidad a la transferencia internacional de datos; Addecco, Randstad Empleo, Manpower., Forsel Grupo Norte, Grupo Crit, etc.

contacto a demandantes de empleo que estén dispuestos a trabajar en otros países[653]. En estos supuestos, el responsable del fichero de datos que se cree con la realización de estas gestiones es la española, lo mismo ocurre con aquellas filiales que la empresa española tenga en otros países cuyo responsable sigue siendo una entidad española; por lo que, en definitiva, estas transferencias se deben realizar atendiendo los requisitos previstos en la normativa sobre protección de datos española.

Como se ha dicho, la búsqueda de empleo en otros países se gestiona también desde el ámbito de la intermediación pública con la red EURES. Es evidente que este sistema de búsqueda de empleo en el extranjero tiene como finalidad propiciar la movilidad profesional de los candidatos que acudan a él y que los ciudadanos puedan consultar las ofertas disponibles en otros países adheridos al sistema. Pues bien, en la política de privacidad de este mecanismo se establecen algunas exigencias sobre la protección de datos de carácter personal de sus usuarios[654].

En primer lugar, es necesario certificar si los datos recogidos a través del sistema EURES son datos de carácter personal, concluyendo que, según lo establecido en la LOPD, esta información cumple con las características pertinentes para tener esa calificación por estar los datos que se solicitan relacionados con la identificación y datos de contacto de su titular y con la información sobre sus antecedentes educativos y profesionales, etc. En segundo lugar, debe comprobarse que la comunicación de información se realiza a países con nivel adecuado de protección, aspecto que parece certificarse al estar el fichero con esos datos ubicado en el Centro de Datos de la Comisión Europea y permitiéndose el acceso tan sólo a los propios los solicitantes de empleo y a todas aquellas empresas constituidas legalmente en el Espacio Económico Europeo.

Los empresarios también pueden utilizar este servicio publicando directamente sus ofertas de empleo y estableciendo las características profesionales que debe tener el candidato que quiera ocupar la vacante

[653] Manpower y Grupo Crit.
[654] Fuente: https://ec.europa.eu/eures/myEures/public/ [Consulta 27/12/2014].

ofertada. Para ello, el empresario tendrá que estar dado de alta en la plataforma EURES y aceptar la política de privacidad del sistema, teniendo así acceso a los datos de los demandantes de empleo que se hayan inscrito en la web, sobre todo los relativos a su trayectoria profesional[655]. La utilización de los datos recogidos en esta plataforma tendrá que respetar los principios de la LOPD, debiendo quedar claro que ese uso tendrá una única finalidad que será la de la búsqueda de empleo para el candidato de empleo que se inscriba en la red EURES, informándole, a su vez, sobre la existencia de esa transferencia internacional de datos para cumplir con el citado objetivo.

En la política de privacidad, por otra parte, se establece que esta información sobre los solicitantes de empleo, o sobre los empresarios registrados, no se revelará a ningún tercero ajeno a la Red EURES, por lo que para poder conocer estos datos es necesaria la previa inscripción en el sistema. Por último, se hace alusión a la conservación de los datos, señalándose que los CV almacenados en el sistema que no han sido ni actualizados ni comprobados por el usuario durante doce semanas dejarán de ser accesibles para los empresarios; mientras que, si pasa un año y no se produce ninguna visita al el perfil del usuario, sus datos serán excluidos del sistema.

También en el ámbito de las TICS, el movimiento internacional de datos ha tenido gran repercusión, pues lógicamente se pueden comunicar datos a terceros que no están en España. Este hecho puede presentar algunos problemas como consecuencia de que, en ocasiones, ni los proveedores de servicios de internet se encuentran en España, ni se informa debidamente a los usuarios de la posibilidad de realizar una transferencia internacional con sus datos. Por ejemplo, los buscadores webs no informan al usuario sobre la

[655] SALAS PORRAS, M.: *El servicio público de empleo y el proceso jurídico de colocación,* Consejo Andaluz de Relaciones Laborales, 2010, pp. 60-61; LÓPEZ-ROMERO GONZÁLEZ, M.P.: "La Red EURES: puesta en contacto de ofertas y demandas de empleo en Europa", *Información laboral. Legislación y convenios colectivos,* núm. 22, 2003, pp. 2-17; ALONSO VEGA, M.T.: "La RED EURES: libre circulación de trabajadores y empleo en la UE", *Boletín asturiano sobre la Unión Europea,* núm. 82-83, 1999, pp. 22-27; GARCÍA MURIAS, R.: "El Programa Erasmus y la Red Eures incidencia en la movilidad académico-profesional en el contexto europeo" en VV.AA.: *Orientación profesional: nuevos escenarios y perspectivas*, Biblioteca Nueva, 2009, pp. 287-304.

posibilidad de que la información contenida en sus bases de datos vaya a ser objeto de alguna transferencia internacional, ni mucho menos los países que van a ser receptores de la misma[656].

Por tanto, el demandante de empleo y usuario del buscador web no conoce dónde van a ir destinados sus datos y tampoco la protección que van a tener. De esta forma se está incumpliendo con el principio de información del art. 5 de la LOPD ya que en el mismo se establece que se tendrá que informar de la identidad del responsable del fichero y, si éste no está ubicado en España, será preciso nombrar un representante para que el interesado pueda ejercer ante él cualquier reclamación[657]. Por este motivo, dentro de la política de privacidad, deben identificarse, por un lado, las entidades a las que van dirigidas esas informaciones de los demandantes de empleo y, por otro, el responsable de la web para poder asegurar la ubicación de ese fichero de datos que se crea con la información de los usuarios, y poder exigir el cumplimiento de lo requerido en la normativa sobre protección de datos si la base de datos no se encuentra en España.

También es muy frecuente que las redes sociales, sobre todo las que de forma más frecuente se utilizan (Facebook, LinkedIn, Xing), no tengan su sede social en España, por lo que el responsable del control de datos es un tercer país. La política de privacidad de la red social LinkedIn establece que: *LinkedIn cumple con el Marco de Puerto Seguro entre EE. UU y la UE[658] según lo estipulado por el Departamento de Comercio de Estados Unidos en lo que se refiere a la recopilación, el uso y la conservación de datos personales de*

[656] En la web infoempleo están trabajando sobre si se incluye en su política de privacidad, la posibilidad de hacer una transferencia internacional de datos pero nada se dice sobre los países que pueden recibir esos datos.
[657] Art. 5 e) de la LOPD: *"De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento".*
[658] Decisión de la Comisión Europea 2000/520/CE, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América [notificada con el número C (2000) 2441].

países miembros de la Unión Europea y Suiza. LinkedIn ha acreditado que se adhiere a los Principios de Privacidad de Puerto Seguro sobre notificación, opción, transferencia ulterior, seguridad, integridad de datos, acceso y aplicación.

Ahora bien, recientemente la Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015[659] ha invalidado y anulado la Decisión 2000/520/CE de la Comisión Europea que cubría la ausencia de tutela de los datos cuando se hacían transferencias a países que no tienen un nivel de protección equiparable a la LOPD, porque entiende que prevalece incondicionalmente y sin ninguna limitación "*la seguridad nacional, el interés público o el cumplimiento de la ley"* sobre los derechos fundamentales a la intimidad y la protección de datos, sin otorgar a los ciudadanos europeos ningún medio para obtener la tutela efectiva de esos derechos; y porque no otorga a los Estados miembros un margen suficiente para suspender las transferencias en caso de que estos apreciaran una vulneración de los derechos de los ciudadanos europeos.

Por su parte, el Tribunal afirma que para que se considere que un país otorga un nivel adecuado de protección su ordenamiento jurídico deberá establecer un nivel de garantías "*esencialmente equivalente"* al establecido en la Unión Europea, ya que sólo así se garantizan suficientemente los derechos fundamentales. La sentencia, cuyas implicaciones marcan un punto de inflexión sobre la forma en la que se realizan las transferencias internacionales de datos a EEUU, reafirma la importancia de la intimidad y la protección de datos, derechos fundamentales que deben gozar de las mayores garantías posibles. Las Autoridades europeas de protección de datos, que ya observaron deficiencias en el Puerto Seguro y las plasmaron en varias cartas y dictámenes, han planificado actuaciones para coordinarse en el análisis de las implicaciones de la sentencia y en las actuaciones nacionales que deban

[659] Disponible en http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d52cb5dc0589b84e368960866f8b1f9746.e34KaxiLc3eQc40LaxqMbN4ObNyNe0?text=&docid=169195&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=82286 [Consulta 7/10/2015].

llevarse a cabo, garantizando una aplicación consistente de la misma en todos los países de la UE[660].

Para terminar, también es preciso atender a la publicación de ofertas de empleo en Internet para juzgar si este hecho se puede considerar un movimiento internacional de datos, teniendo en cuenta que esta publicación puede llegar a usuarios que se encuentran en cualquier rincón del mundo. Si se atiende a la doctrina del TJUE[661], se puede decir que estas publicaciones en internet no se pueden considerar transferencia internacional de datos puesto que entonces no sería legal hacer ninguna divulgación a través de la red debido a que se podría acceder a estos datos desde terceros países, los cuales, en algunos casos, pueden no garantizar el nivel adecuado de protección exigido en la LOPD. Al no considerarse transferencia internacional de datos no tendrían que atender las exigencias contenidas en la normativa sobre protección de datos, permitiendo, el acceso a cualquier información de la red y, en consecuencia, muchas más opciones de búsqueda de empleo en países distintos al de su residencia. No obstante, no puede dejar de indicarse que este hecho puede ir en detrimento de la salvaguarda de los datos como consecuencia de la facilidad que tienen terceros países de conocerlos y procesarlos[662].

---

[660] Fuente: https://www.agpd.es/portalwebAGPD/revista_prensa /revista_prensa /2015/notas_prensa /news/2015_10_06-ides-idphp.php [Consulta 7/10/2015].

[661] Sentencia del TJUE de 6 de noviembre de 2003, Dodi Lindqvist, asunto C-101/01: *"Si el artículo 25 de la Directiva 95/46 se interpreta en el sentido de que existe una «transferencia a un país tercero de datos» cada vez que se publican datos personales en una página web, dicha transferencia será forzosamente una transferencia a todos los países terceros en los que existen los medios técnicos necesarios para acceder a Internet. El régimen especial que prevé el Capítulo IV de la citada Directiva se convertiría entonces necesariamente, por lo que se refiere a las operaciones en Internet, en un régimen de aplicación general. En efecto, en cuanto la Comisión detectara, con arreglo al artículo 25, apartado 4, de la Directiva 95/46, que un solo país tercero no garantiza un nivel de protección adecuado, los Estados miembros estarían obligados a impedir cualquier difusión de los datos personales en Internet. En este contexto, cabe llegar a la conclusión de que el artículo 25 de la Directiva 95/46 debe interpretarse en el sentido de que operaciones como las efectuadas por la Sra. Lindqvist no constituyen, por sí mismas, una «transferencia a un país tercero de datos». Por tanto, no es necesario averiguar si alguna persona de un país tercero ha tenido acceso a la página web de que se trata o si el servidor del proveedor se encuentra físicamente en un país tercero".*

[662] MURILLO DE LA CUEVA, P.L.: *Informática y…*, op. cit., pp. 141-143; ABERASTURI GORRIÑO, U.: "Movimiento Internacional de Datos. Especial referencia a las transferencia internacional…" op.cit., pp. 333-337; GUASCH PORTAS, V.: "Transferencia internacional de datos de carácter personal", *Revista de Derecho de la Uned,* núm. 11, 2012, pp. 9-10.

CAPÍTULO III: PRIVACIDAD Y CONTRATO DE TRABAJO.

SUMARIO: 1. ***INTRODUCCIÓN. 2. DATOS NECESARIOS EN LA RELACIONES DE TRABAJO.*** 2.1. Obtención de datos de carácter personal de los trabajadores. 2.2. Obtención de datos especialmente protegidos de los trabajadores. 2.2.1. Datos relacionados con la salud de los trabajadores. 2.2.2. Datos relacionados con la afiliación sindical. ***3. LICITUD EN EL TRATAMIENTO DE DATOS DE TRABAJADORES EN LA GESTIÓN DE PERSONAL.*** 3.1. Cuestiones generales. 3.2 Tratamiento de datos sanitarios en la relación de trabajo. 3.3. Libertad sindical y tratamiento de datos. **4.** ***OBLIGACIONES Y RESPONSABILIDADES DEL EMPRESARIO RELACIONADOS CON EL CUMPLIMIENTO DE LA LOPD.*** 4.1. Obligaciones del empresario respecto a los datos almacenados en los ficheros empresariales. *4.1.1. Justificación, naturaleza y excepciones. 4.1.2. Tipos de ficheros e inscripción. 4.1.3. Medidas derivadas del principio de seguridad y conservación de ficheros.* 4.2. Aspectos generales acerca de las responsabilidades del empresario respecto a los datos almacenados en los ficheros empresariales. 4.3. Responsabilidad de los ficheros con datos especialmente protegidos de los trabajadores. *4.3.1. Responsabilidad de los ficheros con datos médicos de los trabajadores. 4.3.2. Responsabilidad de los ficheros con datos acerca de la afiliación sindical de los trabajadores.* ***5. LAS CESIONES DE DATOS DE TRABAJADORES EN EL MARCO DE LA RELACIÓN LABORAL.*** 5.1. Mecanismos de transmisión de datos personales de los trabajadores desde la empresa a la Administración Pública. *5.1.1. Requisitos necesarios para la cesión de datos a las Administraciones Públicas. 5.1.2. Características de los ficheros creados en el ámbito de la Administración Pública.* 5.2. Cesiones de datos a los representantes de los trabajadores. *5.2.1. Cesiones de datos a los representantes unitarios. 5.2.2. Cesiones de datos del empresario al sindicato. 5.2.3. Las cesiones de datos del sindicato a la empresa.* 5.3. Las distintas comunicaciones de datos médicos en las relaciones de trabajo.

CAPITULO III: PRIVACIDAD Y CONTRATO DE TRABAJO.

1. INTRODUCCIÓN.

Analizado el derecho a la protección de datos en los procesos de búsqueda de empleo, procede considerar a continuación las posibles vulneraciones de este derecho que se pueden producir tanto a la hora de iniciar una relación laboral como a lo largo de su desarrollo. Lógicamente, la primera información que el empresario conoce del trabajador, además de la facilitada en los procesos de selección de personal, es la objetivamente necesaria para formalizar el contrato de trabajo, la cual, junto a otras que podrán ir prestándose a lo largo de la relación de trabajo, conforman el expediente laboral del trabajador. La obtención de esos datos conlleva casi inevitablemente su tratamiento materializado en su almacenamiento en los ficheros empresariales; lo que constituye una realidad incontestable marcada por la necesidad de gestionar, desde múltiples puntos de vista, las relaciones laborales en el seno de la empresa[663].

Como regla general, la normativa laboral establece que, para la firma de un contrato de trabajo, se tendrán que solicitar obligatoriamente una serie de datos para que ese acuerdo entre empresario y trabajador pueda suscribirse y ser operativo[664]. Puesto que el contrato de trabajo es un pacto entre trabajador y empresario mediante el cual el primero se compromete a prestar un servicio bajo la dirección y organización del segundo a cambio de una retribución económica, es lógico y necesario tener en cuenta en el momento de la contratación circunstancias que afectan a la persona del trabajador y a su capacitación profesional; lo que puede hacer que surjan colisiones entre el derecho del trabajador a la protección de datos y la necesidad objetiva de la empresa de conocer algunos relativos a la edad[665], experiencia, formación y capacidad del trabajador a contratar[666].

---

[663] TASCÓN LÓPEZ, R.: "La protección de datos…" op. cit., pág. 447.
[664] Este aspecto va a ser tratado en el apartado 2 del presente Capítulo.
[665] Lo normal es que el trabajador tenga la edad y capacidad suficiente como para poder firmar un contrato de trabajo, pero pudiera darse el caso de que éste tuviera que estar asistido de un representante legal para ello. La averiguación de estos datos, tiene como finalidad exclusiva el

Todas estas cuestiones, relacionadas con la obtención y tratamiento de los datos personales, tanto al inicio como en el transcurso de la relación laboral, se van a abordar desde cuatro puntos de vista: el primero, el relacionado con la descripción de los datos necesarios para formalizar el contrato de trabajo y el cumplimiento de la LOPD por parte del empresario respecto al tratamiento de datos que realice; en segundo lugar, el análisis de los datos que pueden ir registrándose en los ficheros empresariales durante el desarrollo de la relación de trabajo, profundizando en el tratamiento de los datos especialmente protegidos que tienen repercusión en el ámbito laboral como pueden ser los relacionados con la salud de los trabajadores y con su afiliación sindical; en tercer lugar, la descripción de las obligaciones y responsabilidades del empresario respecto de la información personal y sensible de los trabajadores; y por último, las transmisiones de datos a los diferentes órganos administrativos encargados de los registros de los contratos, normalmente realizadas al inicio de la relación laboral y a través de las plataformas telemáticas creadas al efecto, así como las comunicaciones hechas por el empresario a los representantes de los trabajadores en la empresa con información más o menos personalizada sobre estos últimos.

2. DATOS NECESARIOS EN LAS RELACIONES DE TRABAJO.

La regulación y puesta en práctica del contrato de trabajo crea múltiples vías de obtención de información sobre los trabajadores, tanto por exigencias referidas al interés de las partes, como por la configuración del empresario como un gestor delegado de los poderes públicos; lo que hace que concentre un nivel importante de información que se relaciona directamente con el

comprobar si esa persona puede firmarlo por si misma o necesita la representación legal con la que deben contar las personas con capacidad limitada para contratar.

[666] VV.AA.: *Derecho del Trabajo*, Tecnos, 2014, pp.517-524; GARCÍA VELARDE, M.: "Los elementos esenciales del contrato de trabajo: visión jurisprudencial", *Documentación Laboral*, núm. 45, 1995, pág. 9; APILLUELO MARTÍN, M.: *La relación de trabajo del menor de edad*, CES Madrid, 1999, pp. 62-76. SUAREZ GONZÁLEZ, F.: "La capacidad para contratar. En torno al art. 7" en VV.AA.: *El estatuto de los trabajadores veinte años después*, núm. 100 (Edic. Especial) *Revista Española de Derecho del Trabajo*, Civitas, 2000, pp. 318-322,323-326; MENENDEZ SEBASTIÁN, P.: *Aptitud legal y capacidad en el contrato de trabajo*, CES (España), 2003, pp. 109-116; AMORÓS PÉREZ, F.: " La relación laboral especial de los discapacitados que trabajan en centros especiales de empleo (I): forma del contrato, capacidad para contratar como trabajador, tiempo de trabajo y salario" en VV.AA.: *La aplicación del derecho del trabajo en los centros especiales de empleo,* Tirant lo Blanch, 2009, pp.109-115.

desarrollo de la prestación encomendada al trabajador[667]. Por este motivo, es necesario hacer un recorrido por los datos que identifican al trabajador y que son necesarios para la gestión de personal en la empresa, con el fin de analizar en una segunda instancia si su posterior tratamiento puede atentar contra el derecho a la protección de datos de carácter personal del trabajador. En todo caso, es preciso separar, como se hará, los datos generales de los trabajadores de aquéllos que están dotados de una protección especial como son, por ejemplo, los relativos a su salud y afiliación sindical.

2.1. Obtención de datos de carácter personal de los trabajadores.

De forma sintética puede decirse que, para la redacción del contrato de trabajo, es indispensable, al margen de los propios de la empresa, el conocimiento de los siguientes datos del trabajador: nombre y apellidos; número de afiliación a la Seguridad Social; domicilio; DNI; datos bancarios para proceder al pago de la nómina, y por último, datos y perfil profesional del interesado con la finalidad de certificar su formación y categoría profesional así como la expresión de la valoración empresarial de sus capacidades, aptitudes, habilidades y rendimiento, tras comprobar que las mismas son adecuadas para el desarrollo de las tareas a desempeñar. Junto a estas informaciones también se tienen que tener en cuenta las que, por exigencia de la norma, deben ser objeto de información por el empresario al trabajador y que suelen figurar en el propio contrato o en alguna documentación adjunta[668], como son las referidas a su horario de trabajo, retribución, vacaciones etc.

Especialmente cuidadoso es el tratamiento legal de los números de identificación de los trabajadores, pues constituyen un medio eficaz para adquirir e integrar información relativa a un individuo. Esta cuestión no está contemplada en la LOPD, siendo el RDLOPD el único que hace referencia a

[667] VV.AA: "Protección de datos y contrato de trabajo" *Justicia laboral: revista de Derecho del Trabajo y de la Seguridad Social,* núm. 46, 2011, pág. 24; CARDONA RUBERT, B.: *Informática y contrato…,* op. cit., pp. 101-104.
[668] GARCÍA MURCIA, J. Y MARTÍNEZ MORENO, C.: *Los derechos de información en el contrato de trabajo*, Tirant lo Blanch, 2001, pp. 88-91; RODRÍGUEZ-PIÑERO Y BRAVO FERRER, M.: "El deber del empresario de informar al trabajador de sus condiciones de trabajo" *Revista Relaciones Laborales*, núm. 1, 2000, pp. 277-280. BIBLIOTECA, DICE ALGO MÁS DE OTRAS INFORMACIONES?¿

ella en el art. 5 g) cuando determina que también se considera dato de carácter personal "cualquier información numérica" que sirva para identificar a una persona concreta, como se puede interpretar desde luego que es el DNI o el número de la Seguridad Social. Por su parte, la Directiva 95/46/CE[669] sí tiene previsto el riesgo que supone el libre manejo de los números identificativos desde la perspectiva de la protección de datos y, por este motivo, los incluye en la definición de datos personales -art. 2 a)-[670], instando a los Estados miembros[671] para que determinen en sus legislaciones los requisitos o exigencias concretas para el tratamiento de la información vinculada con los números de identificación personal[672], sobre la base de que, en ocasiones, la utilización de estos identificadores puede llegar a desvelar informaciones de carácter sensible de los trabajadores.

A la hora de formalizar un contrato de trabajo también se pide al trabajador su información académica y profesional, para ver si cumple con las exigencias del puesto de trabajo. Una información se convierte en indispensable cuando lo que se pretende, por ejemplo, es firmar un contrato para la formación[673], unida a la edad que tiene que tener el firmante para poder acceder a esta tipología contractual - entre 16 y 25 años (salvo en los casos de discapacidad o personas pertenecientes a colectivos en situación de exclusión

---

669 HEREDERO HIGUERAS, M.: *La Directiva Comunitaria de Protección de Datos de Carácter Personal*, Aranzadi, 1997, pp. 72-73, 129-131.

670 Art. 2 a) Directiva 95/46/CE: *"Datos personales: toda información sobre una persona física identificada o identificable ("el interesado"); se considera identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".*

671 Art. 8.7 Directiva 95/46/CE: *"Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento".*

672 Sobre el tratamiento del número relativo al DNI vid., Informe jurídico 322/2010 de la AEPD, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informesjuridicos/conceptos/common/pdfs/2010-0322_Tratamiento-del-dato-DNI-y-de-firma-por-representantes-de-empresas.pdf [Consulta 13/08/2015].

673 VV.AA. *Comentarios al Estatuto de los Trabajadores*, Lex Nova, 2014, pp 280-296; LLEO CASANOVA, B.: "Novedades en materia de contratación laboral introducidas por el RD-Ley 4/2013, de 22 de febrero, de medidas de apoyo al emprendedor y de estímulo del crecimiento y de la creación de empleo" *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 34, 2013, pp. 542-545; MARTÍN VALVERDE (COORD.), A.: *Derecho del Trabajo*, Tecnos, 2012, pp. 542-575; CALVO GALLEGO, F.J.: "Modalidades contractuales, dualidad en el mercado y reformas laborales en el bienio 2010 a 2012", *Documentación Laboral*, núm. 94, 2012, pp. 42-44; SEMPERE NAVARRO, A. (COORD.):*El contrato de trabajo*, Aranzadi, 2010, vol. I, pp. 275-278; VV.AA. *Contratación Laboral*, FC editorial, 2008, pp. 89-128.

social[674])-. Además estos trabajadores tienen que carecer de la cualificación profesional reconocida por el sistema de formación profesional para el empleo o por el sistema educativo que sea requerida para concertar un contrato en prácticas. Lo que, no siendo en sí mismo un dato personal, es posible que adquiera esa connotación, que funciona como pararrayos de las normas de protección de datos, si se pone en relación con otras informaciones contenidas en el contrato, contribuyendo a la identificación del trabajador[675].

Durante la existencia de la relación de trabajo el empresario no necesita solicitar muchos más datos al trabajador de los ya registrados para la cumplimentación del contrato de trabajo. Sin embargo, en el transcurso de la vida laboral de ese trabajador en la empresa pueden darse circunstancias que puedan generar nuevas informaciones del trabajador que, desde la perspectiva de la gestión de personal, deban ser incorporadas al correspondiente fichero , ya sea ubicado en el centro de trabajo o en los soportes automatizados creados al efecto.

Estas informaciones pueden estar relacionadas, por ejemplo, con la consecución, por parte del trabajador, de un nuevo título formativo que pueda hacerlo mejorar en su clasificación personal dentro de la empresa; con un cambio de domicilio en dónde poder realizar ahora las notificaciones empresariales o, incluso, con la vigilancia de la actividad laboral en el caso de los teletrabajadores; con la modificación de su situación familiar, la cual va a

[674] Art.11.2 a) ET: *"El contrato para la formación y el aprendizaje tendrá por objeto la cualificación profesional de los trabajadores en un régimen de alternancia de actividad laboral retribuida en una empresa con actividad formativa recibida en el marco del sistema de formación profesional para el empleo o del sistema educativo. El contrato para la formación y el aprendizaje se regirá por las siguientes reglas: a) Se podrá celebrar con trabajadores mayores de dieciséis y menores de veinticinco años que carezcan de la cualificación profesional reconocida por el sistema de formación profesional para el empleo o del sistema educativo requerida para concertar un contrato en prácticas. Se podrán acoger a esta modalidad contractual los trabajadores que cursen formación profesional del sistema educativo. El límite máximo de edad no será de aplicación cuando el contrato se concierte con personas con discapacidad ni con los colectivos en situación de exclusión social previstos en la Ley 44/2007, de 13 de diciembre, para la regulación del régimen de las empresas de inserción, en los casos en que sean contratados por parte de empresas de inserción que estén cualificadas y activas en el registro administrativo correspondiente".*

[675] MORENO VIDA, N.; "Novedades en materia de modalidades contractuales: contrato indefinido para pequeñas empresas, trabajo a tiempo parcial y trabajo a distancia" *Revista Temas Laborales* núm. 115, 2012, pp. 213-215; TARANCÓN PÉREZ, E. Y ROMERO RÓDENAS, M.J.: *Manual de modalidades de contratación laboral*, Bomarzo, 2014.

ser tenida en cuenta no sólo para practicarle las pertinentes retenciones fiscales, sino también para poder solicitar los permisos por maternidad o paternidad[676] y el de matrimonio; con los índices de productividad; con los salarios percibidos; o con la información sobre las fechas de descanso del trabajador, es decir, acerca de las vacaciones solicitadas durante el año, etc.

2.2. Obtención de datos especialmente protegidos de los trabajadores.

2.2.1. Datos relacionados con la salud de los trabajadores.

Los datos de salud recogidos en los reconocimientos médicos, tanto previos como posteriores al inicio de la relación de trabajo, suele variar, incrementándose a partir de las primeras informaciones como consecuencia de la inclusión de todas las necesarias para realizar una correcta política de prevención de riesgos laborales. Algo semejante tiene lugar con los datos relacionados con las bajas por incapacidad laboral que pudiera tener el trabajador, o con otros datos que complementan el estudio de las características médicas del trabajador dependiendo de la tarea que vaya a desempeñar en el centro de trabajo –datos genéticos y realización de test de alcoholemia o drogas[677], por ejemplo-.

Se trata de datos que cobran especial importancia si se tiene en cuenta que los reconocimientos médicos de los trabajadores se configuran como una medida activa y eficaz para que el empresario cumpla con su obligación de vigilar la salud de sus empleados[678], y que, a tenor de lo establecido en el art.

---

[676] Para poder solicitar estos permisos retribuidos por la Seguridad Social, el trabajador necesitará que el empresario expida el correspondiente certificado de empresa, el cual debe contener los datos de la empresa (razón social, CCC, domicilio etc.) y del trabajador (nombre y apellidos, DNI, domicilio, fecha de inicio y finalización del descanso, grupo de cotización etc.). Fuente: http://www.seg-social.es prdi00 /groups/public/documents/binario/113146.pdf.

[677] Así lo manifiesta CARDONA RUBERT, M.B.: "*Deberán ser verdaderamente precisos, sin que puedan realizarse por mero capricho del empresario, contribuyendo a la obtención de dicho fin que en la determinación del riesgo sean utilizados criterios objetivos de valoración. El empresario debe tener en cuenta que los datos que recaen sobre el estado de salud de sus trabajadores sean adecuados, pertinentes y no excesivos en relación con el ámbito laboral",* en *Datos sanitarios y relación laboral*, Tirant lo Blanch, 1999, pág. 25.

[678] Sentencia del Tribunal Constitucional de 15 de noviembre de 2004 (RTC 2004/196); *"El reconocimiento médico en la relación laboral no es, en definitiva, un instrumento del empresario para un control dispositivo de la salud de los trabajadores, como tampoco una facultad que se le reconozca para verificar la capacidad profesional o la aptitud psicofísica de sus empleados con un propósito de selección de personal o similar. Su eje, por el contrario, descansa en un*

22 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales[679], se realizan, sea por el servicio propio de PRL de la empresa, sea por una entidad externa dedicada a esta actividad.

A este efecto, en primer lugar, habrá que determinar la obligatoriedad o no de realizar los citados reconocimientos médicos. La LPRL establece que los reconocimientos médicos se harán, como regla general, siguiendo el principio de voluntariedad, siendo necesario contar, entonces, con el consentimiento del trabajador, sin que su negativa a someterse a ellos pueda generar algún tipo de sanción para el empleado. Sin embargo, y ello es una excepción tan general que casi se convierte en regla, éstos podrían tener carácter obligatorio si tienen como objetivo evaluar[680]: a) los efectos que las condiciones de trabajo hayan provocado en la salud del empleado con el objeto de protegerlos ante el desarrollo de futuras enfermedades degenerativas; b) que estos reconocimientos sean necesarios para certificar si el estado de salud de ese trabajador pude ocasionar un peligro a el mismo o a sus compañeros de trabajo[681]; c) que su realización venga establecida por alguna disposición

---

derecho del trabajador a la vigilancia de su salud. Un derecho que sólo puede venir restringido por las excepciones enunciadas, con los requisitos y límites mencionados. En suma, la regla es –y la regla tiene una clara base constitucional a tenor de la conexión íntima entre los reconocimientos médicos y derechos fundamentales como el de la intimidad personal– la conformidad libre, voluntaria e informada del trabajador para la vigilancia y protección de su salud frente a los riesgos del trabajo."

[679] BOE núm. 269 de 10 de noviembre de 1995.

[680] En algunos supuestos se establece la obligatoriedad de los mismos, siendo la negativa del trabajador motivo para un despido procedente. Tal es así, que en sede jurisprudencial se ha acordado esta solución: Sentencia del Tribunal Superior de Justicia de Extremadura de 5 de febrero de 2013 (AS 2013\246); "*En el supuesto examinado estamos ante la excepción a la voluntariedad en el reconocimiento médico que preceptúa el* artículo 22 *de la LPRL , en el que, además de cubrir los requisitos en el precepto exigidos, tal y como hemos narrado, se ha informado al trabajador por parte del Gerente, y así resulta de la fundamentación jurídica de la sentencia, que la empresa dueña de la obra donde prestaba servicios el actor exigía que los trabajadores que allí prestaban servicios hubieran pasado el oportuno reconocimiento, razón por la que en atención a los hechos declarados probados por la resolución de instancia, no está justificada la negativa del demandante a pasar por el oportuno reconocimiento médico".*

[681] En este sentido vid., la Sentencia del Tribunal Supremo de 10 de junio de 2015 (JUR 2015\180919) en la que se establece la obligatoriedad de los reconocimientos médicos con la finalidad de certificar la idoneidad de un determinado trabajador: *"La interpretación del alcance que poseen las tres excepciones a la regla de voluntariedad no puede prescindir de los criterios sentados al respecto por el Tribunal Constitucional (art. 5.1 LOPJ (RCL 1985, 1578 y 2635)), especialmente contenidos en la STC 196/2004, de 15 de noviembre de 2004 (RTC 2004, 196) . Por ello, de la regulación expuesta deben destacarse los siguientes caracteres y principios: La determinación de una vigilancia periódica -y como regla general consentida-del estado de salud de los trabajadores en función de los riesgos inherentes a su actividad laboral. La voluntariedad del sometimiento a los reconocimientos médicos. La existencia de situaciones*

legal[682]. En consecuencia, sea por la vía voluntaria, sea porque la ley le habilita para ello, lo normal es que el trabajador se someta a los reconocimientos médicos sin que la obtención de estos datos deba considerarse en sí misma como ilícita, pese a su carácter de particularmente sensibles[683].

Entrando en el detalle, el contenido de esos reconocimientos médicos tiene que orientarse a la elaboración de una historia clínico-laboral en la que figuren los datos de «anamnesis[684]», exploración clínica y control biológico; los estudios complementarios en función de los riesgos inherentes al trabajo; una descripción detallada del puesto de trabajo; el tiempo de permanencia en el mismo; los riesgos detectados en el análisis de las condiciones de trabajo y las medidas de prevención adoptadas; además ha de constar, si se dispone de la información, de una descripción de los anteriores puestos de trabajo, los

---

tasadas en las que resulta imprescindible la realización de las exploraciones médicas, limitándose así, excepcionalmente en esos casos, la libre determinación del sujeto. El principio de la indispensabilidad de las pruebas y de su proporcionalidad al riesgo. El necesario respeto del derecho a la intimidad, a la dignidad de la persona y a la confidencialidad de la información relacionada con su estado de salud. El derecho del trabajador a conocer los resultados; la prohibición de utilización de los datos relativos a la vigilancia de la salud con fines discriminatorios o en perjuicio del trabajador. La prohibición de comunicación de la información resultante, salvo que exista consentimiento expreso del trabajador. La posibilidad de transmitir al empresario y a las personas u órganos con responsabilidades en materia de prevención únicamente las conclusiones que se deriven de las exploraciones, y con el exclusivo objeto de que puedan desarrollar sus funciones en materia preventiva".

[682] Vid., art. 22.1 LPRL.

[683] SALAS FRANCO, T. Y ARNAU NAVARRO, F.: *Comentarios a la Ley de Prevención de Riesgos Laborales*, Tirant lo Blanch, 1996, pág. 101; GONZÁLEZ DÍAZ, F.A.: "Una interpretación sobre los límites a la realización de reconocimientos médicos a los trabajadores" *Aranzadi Social*, núm.52, 2011, pp.1-4. TRONCOSO REIGADO, A.: La protección de datos en… op. cit., pp. 467 y ss.; SAN MARTÍN MAZZUCCONI, C.: "La vigilancia del estado de salud de los trabajadores: voluntariedad y periodicidad de los reconocimientos médicos" *Revista del Ministerio de Trabajo y Asuntos Sociales*, núm. 53, 2004, pp.187-197;PEDROSA ALQUÉZAR, S.: *La vigilancia de la salud en el ámbito laboral*, CES, 2005, pp. 20-28; GONZÁLEZ FIERRO, C.: "El deber empresarial de garantizar la vigilancia periódica de la salud de los trabajadores: obligatoriedad versus voluntariedad", *Revista Información Laboral*, núm. 8, 2004, pp. 3-6; BERNARDO JIMÉNEZ, I.: "Vigilancia de la salud de los trabajadores: Los reconocimientos médicos", *Revista Doctrinal Aranzadi Social*, núm. 20, 2003, pp.1-7; NAVARRO NIETO, F.: "Los reconocimientos médicos como instrumentos de vigilancia de la salud laboral: condicionantes legales y jurisprudenciales" *Revista Doctrinal Aranzadi Social,* núm.11, 2012, pp.1-5; TOSCANI JIMÉNEZ, D.: *Reconocimientos médicos de los trabajadores y su régimen jurídico laboral*, Bomarzo, 2011, pp. 85-95; CARRIZOSA PRIETO, E.: "Las facultades de vigilancia y control en el centro de trabajo…", op. cit., pp. 101-105.

[684] Según la Real Academia Española de la Lengua anamnesis significa: "Conjunto de los datos clínicos relevantes y otros del historial de un paciente".

riesgos presentes en los mismos y el tiempo de permanencia en cada uno de ellos[685].

Al margen de que los reconocimientos médicos están protegidos por la exigencia de confidencialidad de las personas que intervienen en su realización[686], hay que hacer una distinción entre los datos que se obtienen de los exámenes médicos, ya que no todas estas informaciones médicas pueden ser conocidas por el empresario y, en consecuencia, tampoco almacenadas posteriormente. Así, por un lado, están los resultados en sentido estricto, concebidos como la información relativa a la salud del trabajador, derivada de las distintas pruebas realizadas para certificar los efectos que el desempeño de su puesto de trabajo puede tener en su salud; y, por otro lado, las conclusiones en las que el empresario obtiene información relativa, simplemente, a la aptitud o inaptitud del trabajador para el desempeño de un determinado puesto de trabajo[687] y aquellos datos referidos a las incidencias que se pueden dar en el centro de trabajo relacionadas con la salud de los trabajadores[688]. No es que los primeros no puedan ser tratados desde el punto de vista del almacenamiento de la información, sólo que, desde el inicio, el acceso a los mismos está fuertemente protegido; mientras que las conclusiones (tanto generales como referidas a un trabajador concreto), son accesibles a la empresa y, por tanto, susceptibles de tratamiento posterior en términos más flexibles.

---

[685] Art. 37.3 c) del RD 39/1997, de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención (BOE núm. 27 de 31 de enero de 1997).
[686] Art. 22.2 de la LPRL: *"Las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo respetando siempre el derecho a la intimidad y a la dignidad de la persona del trabajador y la confidencialidad de toda la información relacionada con su estado de salud".*
[687] Vid., art. 22. 3 y 4 de la LPRL.
[688] Art. 23.1. d) y e) de la LPRL: *"1. El empresario deberá elaborar y conservar a disposición de la autoridad laboral la siguiente documentación relativa a las obligaciones establecidas en los artículos anteriores: d) Práctica de los controles del estado de salud de los trabajadores previstos en el artículo 22 de esta Ley y conclusiones obtenidas de los mismos en los términos recogidos en el último párrafo del apartado 4 del citado artículo. e) Relación de accidentes de trabajo y enfermedades profesionales que hayan causado al trabajador una incapacidad laboral superior a un día de trabajo. En estos casos el empresario realizará, además, la notificación a que se refiere el apartado 3 del presente artículo".*

En otro orden de cosas, también se pueden conocer datos médicos de los trabajadores cuando solicitan una baja por incapacidad que le impida, temporal o de forma permanente –ya sea por enfermedad común, profesional o accidente de trabajo-, realizar sus funciones en la empresa. No obstante, y según lo establecido en las normas reguladoras de esta materia, en los partes de baja se incluye sólo el diagnóstico, la limitación de la capacidad del trabajador y el pronóstico sobre la duración de la baja[689].

Se trata de una información que será facilitada por el médico del Servicio Público de Salud o Mutuas Colaboradoras con la Seguridad Social (en adelante, MCSS) y será transmitida de forma íntegra al Instituto Nacional de la Seguridad Social o a la entidad colaboradora que, como se verá[690], además de los profesionales sanitarios, tienen la facultad de crear un fichero con esa información médica del trabajador. No obstante, en estos casos, la empresa no accede a una información detallada sobre la salud de los trabajadores ya que en la copia del parte médico que se le entrega no aparece nada que pueda revelar algún dato sensible del trabajador por lo que, en este sentido, el acopio de esa información por parte del empresario no afecta a las reglas de protección de datos de salud.

En cuanto a la información acerca del código genético del trabajador en el marco de la relación de trabajo[691], estas informaciones se deben considerar, lógicamente, datos sobre la salud y, por tanto, especialmente sensibles[692]. Por último, otra forma de captar datos relacionados con la salud de los trabajadores

[689] Art. 1.2. del RD 575/1997, de 18 de abril, por el que se regulan determinados aspectos de la gestión y control de la prestación económica de la Seguridad Social por incapacidad temporal (BOE núm. 98 de 24 de abril de 1997) :"*Todo parte médico de baja irá precedido de un reconocimiento médico del trabajador que permita la determinación objetiva de la incapacidad temporal para el trabajo habitual, a cuyo efecto el médico requerirá al trabajador los datos necesarios que contribuyan a precisar la patología objeto de diagnóstico. En todo caso, el original del parte de baja y la copia a remitir a la Entidad Gestora o, en su caso, a la Mutua de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social deberán contener el diagnóstico y la descripción de las limitaciones en la capacidad funcional del trabajador, así como una previsión de la duración del proceso patológico".*

[690] Vid., apartado 5.3 del presente Capítulo.

[691] SÁNCHEZ-CARO, J. Y ABELLÁN, F.: *Datos de salud y datos genéticos: su protección en la Unión Europea y en España*, Comares, 2004, pág.18.

[692] Documento de trabajo del Grupo del art. 29 sobre datos genéticos (12178/03/ES, WP 91) adoptado el 17 de marzo de 2004, disponible en: www.europa.eu.int/comm/privacy (Consulta 25/11/2015).

puede ser la derivada de los controles médicos relativos al consumo de alcohol y drogas; datos que pueden ser imprescindibles, a tenor de la actividad concreta, para comprobar si el trabajador acude a su centro de trabajo sin estar bajo los efectos de alguna sustancia que pueda interferir en su capacidad para realizar la tarea encomendada.

2.2.2. Datos relacionados con la afiliación sindical.

Siguiendo con los datos especialmente protegidos es necesario hacer alusión a aquellas informaciones que pueden desvelar la afiliación sindical del trabajador. Por un lado, son, lógicamente, las organizaciones sindicales las que, en un primer momento, manejan datos de esta naturaleza; pero, y en lo que al ámbito empresarial se refiere, el empresario puede también tratar datos relacionados con la afiliación o la actividad sindical de los trabajadores. En unos casos en virtud de compromisos convencionales para el descuento de la cuota sindical [693]; en otros, para, por ejemplo, descontar del salario los días en los que haya permanecido en situación de huelga[694].

El empresario también puede conocer, y posteriormente archivar, estas informaciones a efectos organizativos si, por ejemplo, el trabajador pudiera ser beneficiario del crédito horario que le corresponde para ejercer sus funciones de representante sindical[695]; o si el empresario tuviera que asegurar el cumplimiento de los servicios esenciales durante los días de huelga. Obviamente, todas estas informaciones, o bien provienen del propio trabajador o del sindicato en el que éste se encuentre afiliado (dando lugar, en este segundo supuesto, a una cesión de datos de las descritas en apartados

[693] Art. 11.2 de la Ley 2/1985, de 2 de agosto, de Libertad Sindical (BOE núm. 189 de 8 de agosto de 1985): *"El empresario procederá al descuento de la cuota sindical sobre los salarios y a la correspondiente transferencia a solicitud del sindicato del trabajador afiliado y previa conformidad, siempre, de éste".*

[694] Art. 6.2 y 3 del RDL 17/1977: "*2. Durante la huelga se entenderá suspendido el contrato de trabajo y el trabajador no tendrá derecho al salario. 3. El trabajador en huelga permanecerá en situación de alta especial en la Seguridad Social, con suspensión de la obligación de cotización por parte del empresario y del propio trabajador. El trabajador en huelga no tendrá derecho a la prestación por desempleo, ni a la económica por incapacidad laboral transitoria".*

[695] Art. 37.3 e) del ET: *"El trabajador, previo aviso y justificación, podrá ausentarse del trabajo, con derecho a remuneración, por alguno de los motivos y por el tiempo siguiente: e) Para realizar funciones sindicales o de representación del personal en los términos establecidos legal o convencionalmente".*

sucesivos del presente trabajo[696]), o bien son consecuencia del ejercicio por parte del trabajador de determinados derechos colectivos cuyo conocimiento es inevitable por parte de la empresa. Esto en lo que se refiere a su obtención, ya que otra cosa es el tratamiento de tales datos, como se verá a continuación.

3. LICITUD EN EL TRATAMIENTO DE LOS DATOS DE TRABAJADORES EN LA GESTIÓN DE PERSONAL.

Evidentemente, todos estos datos de carácter personal del trabajador a que se ha hecho referencia son precisos para formalizar y mantener la relación laboral, pero su protección no se atendría a las reglas de la LOPD si no fueran archivados en los registros empresariales.

3.1. Cuestiones generales.

En cumplimiento del *principio de calidad* el procesamiento de esos datos por parte del empresario tiene que ser adecuado, pertinente y no excesivo para la finalidad para la que se solicitan. Algunos autores[697] han establecido un interesante debate sobre los términos adecuación y pertinencia de los datos, si bien puede decirse que, , en materia laboral, se debe atender, por un lado, a la cantidad de datos necesarios para lograr la finalidad legítima pretendida por el empresario (en este caso, administrar el personal de su empresa) y, por otro, a la exigencia de no pedir y tratar más información de la necesaria para identificar a cada trabajador, en los términos amplios antes dichos[698].

---

[696] Sobre el tratamiento de datos relacionados con el ejercicio de la actividad sindical véase apartado 3.2. y 5.2.2. del presente Capítulo.

[697] Así MURILLO DE LA CUEVA, P.L. mantiene que adecuaciòn son tèrminos sinònimos pero con matices que hacen referencia a la idoneidad de los datos respecto a la finalidad del fichero de datos, en MURILLO DE LA CUEVA, P.L.: *Informatica y...*op. cit., pág. 65; HERRÁN ORTIZ establece que la adecuaciòn hace referencia a la conexiòn del dato con la finalidad mientras que la pertinencia con la necesidad de no solicitar màs datos de los necesarios para cumplir el objetivo, en HERRÁN ORTIZ, A.I.: *La violación de la intimidad en la protecciòn de datos personales*, Dykinson, 1999, pág. 243; SERRANO PÉREZ, establece que los conceptos adecuaciòn y pertinencia no se solapan, sino que establecen matices diferentes para aludir a la cantidad y calidad de los datos, en SERRANO PÉREZ, M.:*El derecho fundamental a la protecciòn de datos*, Civitas, 2003, pp. 437-443.

[698] Vid. apartado 2 del presente Capítulo.

Siguiendo estos criterios y en lo que a los datos iniciales precisos para cumplimentar el contrato de trabajo y la observancia del principio de calidad se refiere, existen situaciones en las que el conocimiento de algunas informaciones es imprescindible. Por ejemplo, la información relativa al domicilio de los trabajadores, sobre todo para que el empresario pueda comunicarse con ellos e, incluso, si tiene previsto abonar alguna dieta relacionada con el traslado al centro de trabajo. A su vez, existen empresas[699] que ofrecen un servicio de transporte a sus empleados y, en este caso, conocer el dato del domicilio particular del trabajador es primordial para poder fijar los distintos puntos de recogida de los mismos. Por tanto, su almacenamiento en las bases de datos empresariales es legítimo y cumple la exigencia de calidad sin que, no obstante, puedan utilizarse para otros fines.

Acerca de la posibilidad de recopilar y tratar los datos bancarios de los trabajadores, el archivo de estas informaciones se justifica cuando el pago del salario se realiza mediante transferencia bancaria, no siendo necesario ni respetuoso con el principio de calidad el registro de esos datos si ese abono se realiza a través de otros medios, como por ejemplo, pudiera ser un cheque bancario. No tiene sentido, entonces, la recogida de este dato con el objetivo de pagar la nómina del trabajador si no se va a hacer uso de la cuenta bancaria para ello[700].

Ahora bien, existen una serie de datos cuya solicitud y almacenamiento puede considerarse innecesaria y no pertinente para la correcta gestión de los recursos humanos de la empresa. Por ello, recientemente el Tribunal Supremo en su Sentencia de 21 de septiembre de 2015[701] ha considerado abusiva la cláusula contractual en la que se obliga al trabajador a ofrecer su teléfono móvil personal o email para que el empresario se ponga en contacto con él por medio

[699] Empresas como Abengoa (Sevilla), Pitalmeria (Almería), Airbus (Sevilla), Bankinter (Madrid), etc.
[700] Por ejemplo, si el contrato que se va a firmar en un contrato de trabajo en grupo (art. 10 del ET) el empresario tiene que identificar a todos los miembros de ese grupo de trabajo creado para trabajar de forma colectiva, a efectos, de la retribución. Pues, el abono por la tarea encomendada se realiza al grupo de forma global y, entonces, será el responsable del grupo el encargado de solicitar los datos bancarios de cada integrante con el objetivo de distribuir de forma equitativa o proporcional el sueldo a cada trabajador.
[701] Sentencia del Tribunal Supremo de 21 de septiembre de 2015 (JUR 2015\239514).

de estos mecanismos. El problema que se plantea está relacionado con la obligatoriedad que presenta la cláusula pues, el Supremo si admite que estos datos puedan ofrecerse a la empresa pudiendo incluso "*resultar deseable, dado los actuales tiempos de progresiva pujanza telemática en todos los ámbitos*".

Una cosa es que la lógica de las relaciones de trabajo pueda, en un determinado momento, hacer necesario el manejo de los datos relativos al teléfono móvil y correo electrónico, pero cosa distinta ocurre cuando la petición y posteriormente archivo de esos datos se presenta como obligatoria a la hora de la firma del contrato de trabajo[702], ya que no se considera un dato esencial para cumplir el objetivo del trabajo. De hecho si de la comunicación a través de estos medios con el trabajador dependiera el buen desarrollo de la actividad empresarial, lo lógico sería que el propio empleador facilitará esos instrumentos y no se utilizaran para ello aquellos personales del trabajador.

Al formalizar un contrato, el empresario también necesita de una información referida a la formación, capacitación y experiencia profesional del trabajador; información que suele ser tratada y almacenada a efectos de la gestión del personal y que es pertinente y no excesiva en cuanto a las exigencias del principio de calidad[703]. Puesto que el objetivo pretendido por el empresario con la solicitud y el almacenamiento de estos datos formativos está relacionado con la clasificación profesional de ese trabajador en la empresa, la inclusión y el seguimiento de estos datos en los ficheros empresariales con esa intención de identificación profesional en función del trabajo a desempeñar resulta adecuada no sólo con el objetivo de conocer el curriculum profesional

[702] Sentencia del TS de 21 de septiembre de 2015 (JUR : *"La contestación -sucinta- a tales planteamientos viene dada por la normativa y doctrina constitucional más arriba indicadas [FJ segundo.1 y 2]: a) el ámbito de la protección va más allá de la intimidad que protegen el art. 18.1 CE (RCL 1978, 2836) y la LOPD, alcanzando la expresión «datos de carácter personal» a «cualquier información concerniente a personas físicas» [art. 3.a) LOPD]; y b) lo que el derecho fundamental protege no solamente es la utilización -indebida- de los datos, sino su propia adquisición… Como oportunamente indica el razonado informe del Ministerio Fiscal, «[n]os encontramos ante unos datos de carácter personal, cuyo conocimiento, uso y destino tiene que quedar bajo el control de su titular".*

[703] En cambio, si el acuerdo laboral que va a firmar el trabajador es un contrato en prácticas (art. 11.1 del ET), la solicitud de los datos formativos es indispensable puesto que estos contratos sólo pueden realizarlos aquellos ciudadanos que estén en "*posesión de título universitario o de formación profesional de grado medio o superior o títulos oficialmente reconocidos como equivalente.*

del trabajador a los efectos de la asignación de tareas sino también para que el empresario pueda, por ejemplo, ofrecer a los trabajadores la posibilidad de participar en las actividades formativas que organice[704].

Una necesidad informativa y de tratamiento que se suscita igualmente a la hora de suscribir y desarrollar un contrato formativo (sea en formación o en prácticas[705]) donde el conocimiento y archivo de la información relativa a una concreta situación formativa, de exclusión social o acerca del grado de discapacidad de la persona que se va a contratar no es contrario al principio de calidad de los datos pues el empresario puede justificar que esa captación de información del trabajador[706] se hace precisa para poder certificar, por ejemplo, que estos trabajadores no necesitan cumplir con el criterio de edad (entre 16 y 25 años) para suscribir un contrato en prácticas o que puede beneficiarse de determinadas ventajas a la hora de contratar a estos trabajadores. Pero es evidente que el empresario sólo puede tratar esos datos para las gestiones relativas a la contratación del trabajador así como para crear la correspondiente bases de datos de trabajadores con estas cualidades, siempre que ello no suponga un tratamiento que no se adecue a la finalidad pretendida, que es la

[704] En este sentido el art. 4.2 LOPD que sustituye al art. 4.2 de la LORTAD se presenta màs permisivo, ya que, el tèrmino incompatible puede admitir el tratamiento de datos para situaciones que sean acordes con la finalidad originaria de la recogida. Lo decisivo es que el nuevo uso se justifique, también, en función del contrato de trabajo y que el trabajador sea debidamente informado para que pueda ejercer sus derechos.

[705] Art.11.2 a) ET: *"El contrato para la formación y el aprendizaje tendrá por objeto la cualificación profesional de los trabajadores en un régimen de alternancia de actividad laboral retribuida en una empresa con actividad formativa recibida en el marco del sistema de formación profesional para el empleo o del sistema educativo. El contrato para la formación y el aprendizaje se regirá por las siguientes reglas: a) Se podrá celebrar con trabajadores mayores de dieciséis y menores de veinticinco años que carezcan de la cualificación profesional reconocida por el sistema de formación profesional para el empleo o del sistema educativo requerida para concertar un contrato en prácticas. Se podrán acoger a esta modalidad contractual los trabajadores que cursen formación profesional del sistema educativo. El límite máximo de edad no será de aplicación cuando el contrato se concierte con personas con discapacidad ni con los colectivos en situación de exclusión social previstos en la Ley 44/2007, de 13 de diciembre, para la regulación del régimen de las empresas de inserción, en los casos en que sean contratados por parte de empresas de inserción que estén cualificadas y activas en el registro administrativo correspondiente".*

[706] VV.AA.: Principios *y derechos de la protección de datos de carácter personal. Doctrina de la Agencia de Protección de Datos de la Comunidad de Madrid.* Thomson-Civitas, 2010, pp. 223-224.

de contratar al trabajador con un contrato con finalidad formativa y de promoción de empleo de determinados colectivos[707].

Todos estos datos, cuando han sido registrados en los ficheros empresariales, tendrán normalmente que ser puestos al día ya que desde el inicio de la relación laboral se han podido producir modificaciones que deben estar recogidas en el fichero. A estos efectos, por ejemplo, se pueden producir cambios de la cuenta bancaria dónde realizar el pago del salario, sobre el nivel formativo del trabajador si es que ha completado o mejorado su formación a los efectos del desempeño de su puesto u otro de superior categoría; sobre su estado civil y carga familiar o sobre el nuevo domicilio.

Relacionada con la actualización de datos en los ficheros empresariales se presenta la eliminación de la base de datos de los datos inexactos que ya no ofrezcan una información acorde con la realidad de ese trabajador. Obviamente, el mantenimiento de estos datos incompletos en los ficheros empresariales puede suponer un riesgo de lesión en su posición jurídica en la medida en que, sobre el almacenamiento erróneo de informaciones personales, pueden adoptarse decisiones empresariales que pueden llegar a provocar un perjuicio para el trabajador. Por ejemplo, no ofrecerle al trabajador un puesto con más responsabilidad en la empresa por desconocer su nueva formación; o hacerle transferencia de su nómina a una cuenta bancaria de la que ya no es titular. Aunque normalmente será el propio trabajador el primer interesado, y obligado, a comunicar estos cambios al empresario.

Otro de los principios que tiene que cumplir el empresario para tratar los datos de forma diligente es el *principio de información*. De forma que todos los

[707] Art. 11.2 d) del ET: *"El trabajador deberá recibir la formación inherente al contrato para la formación y el aprendizaje directamente en un centro formativo de la red a que se refiere la disposición adicional quinta de la Ley Orgánica 5/2002, de 19 de junio, de las Cualificaciones y de la Formación Profesional, previamente reconocido para ello por el Sistema Nacional de Empleo. No obstante, también podrá recibir dicha formación en la propia empresa cuando la misma dispusiera de las instalaciones y el personal adecuados a los efectos de la acreditación de la competencia o cualificación profesional a que se refiere el apartado e), sin perjuicio de la necesidad, en su caso, de la realización de periodos de formación complementarios en los centros de la red mencionada. La actividad laboral desempeñada por el trabajador en la empresa deberá estar relacionada con las actividades formativas. La impartición de esta formación deberá justificarse a la finalización del contrato".*

trabajadores deben conocer el sentido de la petición de esos datos de carácter personal y, por supuesto, si van a ser registrados en los ficheros empresariales;/ información que debe suministrar el empresario.

Este derecho del titular del dato, el trabajador, a ser informado sobre que tratamiento se le va a dar a los datos comunicados al empresario tiene más importancia, si cabe, en materia laboral, viciando la posible ausencia de esas advertencias la misma declaración de voluntad del trabajador al consentir su tratamiento. Este derecho a la información funciona, sin duda, como una garantía para los trabajadores puesto que se les tendrán que informar también sobre los derechos que tienen respecto de los datos suministrados y ante quién puede ejercerlos[708]. Así la AEPD establece que el contrato de trabajo puede ser un medio adecuado para facilitar al empleado toda la información referida al tratamiento de sus datos de carácter personal[709].

En este sentido, existen resoluciones judiciales en las que se entiende vulnerado el derecho a la protección a los datos de identificación del trabajador cuando el empresario los ha pedido sin proporcionarle la información debida para tratarlos[710]. No obstante, si se analizan con detalle los modelos de

[708] AEPD.: *La protección de datos en las relaciones laborales*, 2009, pág.8; CARDONA RUBERT, M.B.: *Informática y contrato…,* op. cit., pág. 127.
[709] AEPD: *La protección de datos…*op. cit*.,* pp.10-11; TASCÓN LÓPEZ, R.: "La protección de datos…" op. cit., pp. 490-491; SEMPERE NAVARRO, A.V.: "Contrato laboral y tecnologías novedosas", *Actualidad Jurídica Aranzadi* núm. 912, 2015.
[710] Sentencia de la Audiencia Nacional de 30 de noviembre de 2001 (ROJ: SAN 7179/2001); "*La recogida de la información se efectuó por medio de una ficha manual que incluye para su cumplimentación los siguientes apartados: franquicia de, nombre, apellidos, DNI, fecha de nacimiento, domicilio, avisar en caso de accidente a, teléfono, departamento, autónomo nº y fotografía, ficha diseñada y generada por SEUR y remitida a todas las franquicias para que recabaran los datos a sus empleados. La citada ficha no incluye información sobre la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean formuladas, de las consecuencias de la obtención de datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación cancelación y de la identidad y dirección del responsable del fichero….la Ley exige que la actividad informativa sea más precisa y se ponga en conocimiento de los afectados, además de la existencia del fichero y de su finalidad, del carácter obligatorio o facultativo de su respuesta, de las consecuencias de esa obtención de datos o de su negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación cancelación y, por último, de la identidad y dirección del responsable del fichero. Nada de esto se hizo por la recurrente, ni siquiera se ha acreditado que esa pretendida información que hizo por sí misma, o que solicitó a otros a suministrar, llegó a conocimiento de todas y cada una de las personas a quienes se obligaba a rellenar la ficha en cuestión".*

contratos oficiales proporcionados por Ministerio de Empleo y Seguridad Social es curioso observar que en ellos[711] se informa de que los datos están sometidos a lo que establezca la LOPD, pero no mencionan ni al RDLOPD, ni comentan con más detalle el tratamiento que se le va a dar a esos datos, ni tampoco quién va a ser el responsable del fichero, incumpliendo por ello lo establecido en el art. 5.1 LOPD[712]. Aunque en el formulario de contratación no se tenga en cuenta, de forma precisa y detallada, lo establecido en la LOPD, es evidente que esta información la tiene que otorgar el empresario ya que va a ser quien la procese, pudiendo cumplir con su obligación informativa sea en el propio contrato como en un documento anexo al mismo en el que se ponga de manifiesto la política de privacidad aplicada por la empresa.

Por último hay que hacer mención al cumplimiento del *principio del consentimiento* a la hora de tratar estos datos. En primer lugar, sobre el significado del consentimiento inequívoco que, de forma genérica, se establece para el tratamiento de datos definido y regulado en los arts. 3 h) y 6 de la LOPD, se puede decir que en el ámbito laboral esta regla del consentimiento pasa a un segundo plano puesto que la LOPD establece que éste no será preciso si el procesamiento de la información tiene como pretensión el mantenimiento o cumplimiento de una relación laboral entre las partes de un contrato o precontrato, en este caso, de trabajo[713]. Siendo obvio que los datos facilitados por el trabajador al empresario en el transcurso de su relación de trabajo son imprescindibles para cumplimentarlo y, por tanto, están relacionados básicamente con el inicio de la relación laboral; pero también en relación con los que se generen a lo largo de la relación laboral.

---

[711] Fuente: http://www.sepe.es/contenido/empleo_formacion/empresas/contratos_trabajo/.

[712] Es cierto que en la LOPD no se establece ninguna forma para dar esa información sobre el tratamiento de los datos del ciudadano, pero según lo establecido en el art.18 del RDLOPD; "*El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/ 1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado."* Tan sólo se exige que se informe del contenido del art. 5 de la LOPD, pero nada se dice sobre la forma de acreditar el cumplimiento de este deber, es por ello, que se podrá informar al trabajador de forma verbal, aunque sea más complicado demostrar que el responsable del fichero ha cumplido con la obligación de información.

[713] Art. 6.2 LOPD.

En todo caso, la dispensa del consentimiento del trabajador es relativa ya que abarca solo los datos genéricos necesarios, en este caso, para el mantenimiento del acuerdo laboral; por lo que no se podrán tratar sin consentimiento del trabajador otros datos que pudieran llegar a archivarse y que no persigan este objetivo, por ejemplo los relacionados con su situación familiar, con su formar de proceder en el trabajo (listas negras)[714], datos relativos al email o teléfono móvil particular[715], etc. Por tanto, no podrán realizarse tratamientos de datos sin consentimiento del trabajador si éstos exceden de la finalidad de mantener la relación de trabajo[716], por lo que, si se

[714] Sobre este aspecto vid., apartado 3.3 del capítulo IV.

[715] Sentencia de la Audiencia Nacional de 28 de enero de 2014 (AS 2014\231) establece; "*Teniendo en cuenta lo que se acaba de indicar, la comunicación de los números de teléfono móvil y dirección de correo electrónico requerirá el consentimiento de los interesado a menos que la misma pueda ampararse en alguno de los supuestos excepcionados por el citado artículo 6.2, y ninguno de los cuales parece concurrir en el supuesto contemplado, por lo que la empresa no puede imponer a los trabajadores que le faciliten los referidos datos porque ello sería contrario a la Ley 15/1999 . En consecuencia, conforme a lo expuesto, nos encontramos ante un derecho fundamental, la protección de datos de carácter personal, que es distinto de los garantizados en el artículo. 18.1 de la Constitución (RCL 1978, 2836) y que se reconoce como titular del mismo a las personas físicas, tal y como se reconoce tanto en la LOPD como en la Directiva 95/46 (LCEur 1995, 2977) así como en Convenios Internacionales suscritos por España cuya comunicación y tratamiento exige el consentimiento del titular Resulta cláusula abusiva aquella que se apoya en una circunstancia sobre cuya concurrencia no puede ejercer ninguna influencia la conducta del trabajador y sí, en cambio, la de la empresa";* En el mismo sentido la Sentencia del TS de 21 de septiembre de 2015 *(*JUR 2015\239514*),* no comparte que en el contrato de trabajo se haga constar mediante cláusula/tipo que el trabajador presta su «*voluntario*» consentimiento a aportar los referidos datos personales, ya que esta voluntariedad es ficticia como consecuencia de que el trabajador es la parte más débil del contrato de trabajo y está dispuesto a dar esos datos si el empresario así se lo manifiesta: *: "Tampoco podemos aceptar el distorsionado planteamiento que de la cuestión litigiosa hace el recurso, cuando argumenta que a nadie se le impone ni la adquisición de los instrumentos para proporcionar los datos en cuestión [teléfono móvil; ordenador personal] ni la obligada aportación de los datos [número de teléfono y cuenta de correo]; y que el clausulado evidencia la voluntariedad de su aportación. Este Tribunal en absoluto niega que voluntariamente puedan ponerse aquellos datos a disposición de la empresa, pues ello es algo incuestionable; es más, incluso pudiera resultar deseable, dado los actuales tiempos de progresiva pujanza telemática en todos los ámbitos. A lo que exclusivamente nos oponemos es que en el contrato de trabajo se haga constar -como específica cláusula/tipo- que el trabajador presta su «voluntario» consentimiento a aportar los referidos datos personales y a que la empresa los utilice en los términos que el contrato relata, siendo así que el trabajador es la parte más débil del contrato y ha de excluirse la posibilidad de que esa debilidad contractual pueda viciar su consentimiento a una previsión negocial referida a un derecho fundamental, y que dadas las circunstancias -se trata del momento de acceso a un bien escaso como es el empleo- bien puede entenderse que el consentimiento sobre tal extremo no es por completo libre y voluntario [sobre tal extremo, aunque referido a cláusulas de temporalidad, SSTS 20/01/98 (RJ 1998, 1000) -rcud 317/97 -; 30/03/99 (RJ 1999, 3775) -rcud 2815/98 -; 29/05/00 (RJ 2000, 4804) -rcud 1840/99 -; y 18/07/07 (RJ 2007, 6738) -rcud 3685/05 -]; de forma que la ausencia de la menor garantía en orden al consentimiento que requiere el art. 6.1 LOPT, determinó precisamente que la sentencia recurrida -y ahora esta Sala- consideren que tal cláusula es nula por atentar contra un derecho fundamental, y que debe excluirse de los contratos de trabajo".*

[716] Sentencia del Tribunal Supremo (Sala Social) de 27 de octubre de 2010 (RJ 2010\8461), en la que no se admite las excepción al consentimiento para justificar la remisión de datos

pretende utilizar los datos obtenidos por el empresario con otros objetivos distintos al citado mantenimiento, será necesario que el trabajador muestre su conformidad a través de la prestación del consentimiento[717], inequívoco, libre y específico, y que se le informe del nuevo uso que se le va a dar a la información que le concierne[718].

---

médicos del trabajador: *"Las previsiones del Convenio en esta materia , si se entienden referidas al contenido de los reconocimientos, no se ajustan a las exigencias derivadas del respeto a la intimidad y esta invasión de la intimidad no puede justificarse en el presente caso en el función del consentimiento del trabajador. En primer lugar, porque no hay ningún interés general que justifique el que se recaben estos reconocimientos médicos confidenciales, se hagan constar en una tarjeta profesional y se remitan a un organismo paritario -la Fundación Laboral Construcción- que no tiene una configuración técnico-sanitaria. La remisión de estos datos carece de interés en términos tanto sanitarios, como de prevención, pues lo importante es que los reconocimientos se realicen y que sus conclusiones se tengan en cuentan por el empresario y los órganos competentes en materia de prevención para adoptar las medidas de protección oportunas, lo que ninguna relación tiene con la remisión de esos reconocimientos a un organismo paritario sin ninguna finalidad específica en orden a la adopción de medidas preventivas en atención al contenido de los reconocimientos y muchos menos con la mera circulación de esa información en una tarjeta profesional. La única función a la que parece apuntar esa ruptura de la confidencialidad a través de la circulación de los reconocimientos sería el objetivo de evitar la repetición de los informes en caso de rotación (artículo 130 .d) del Convenio), lo que es contrario a la doctrina de la STC 70/2009 (RTC 2009, 70) . En segundo lugar, porque el consentimiento del trabajador a la hora de proporcionar esta información puede verse perturbado por las consecuencias que la negativa a aportar los informes pueda tener sobre sus posibilidades de ser contratado a partir de la posible clasificación de los trabajadores distinguiendo entre quienes aportan los reconocimientos y los que no lo hacen. Las consideraciones anteriores afectan lógicamente al contenido de los reconocimientos médicos, pero no al mero dato que se limita a constatar que éstos se han realizado sin aportar información sobre su contenido o resultados. No es, por tanto, necesario anular las referencias que se contienen en el apartado c) del art. 160, en el apartado c) del número 4 del art. 163 y en el modelo de solicitud del Anexo V , siempre que se entienda que informan sobre la mera existencia de los reconocimientos sin constancia, registro, certificación o expresión de su contenido. Debe, sin embargo, anularse la mención contenida en el inciso final del art. 130 .d), sobre las propuestas relativas a la forma de evitar la repetición de los reconocimientos de los trabajadores de alta rotación, porque para evitar esa repetición de los informes sería necesario el conocimiento de su contenido".*

[717] Existe una corriente doctrinal que ha considerado que el principio de calidad está intrínsecamente unido al del consentimiento vid., FERNÁNDEZ VILLAZÓN, L.A.: "Los derechos de los trabajadores frente al tratamiento de datos personales. Comentario a la directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos", *Relaciones Laborales*, núm. 2, 1996, pág. 1187-1188; TASCÓN LÓPEZ, R.: "La protección de datos…", op. cit., pp. 472-473.

[718] En algunos supuestos no se admite la vulneración del derecho a la intimidad del trabajador, fundamentando su pretensión en que será necesario el conocimiento de los datos identificativos del vendedor en aras a poder dirigirse a él para una determinada atención reclamación que pudiera surgir. Tal es así, que el Tribunal Supremo en su Sentencia de 18 de diciembre de 2006 (RJ 2007/750) establece; "*Tales* datos *consignados en el resguardo coinciden con los facilitados en la placa cuando ésta se porta por el trabajador (lo cual queda a elección de la persona afectada), aun cuando sea cierto que tales* datos *personales contenidos en la placa de identidad no se trasladan físicamente por su uso a terceros, que no son indeterminados sino aquellos que guardan con la empresa la relación de clientes. Cabe también discutir que, si por la naturaleza del trabajo contratado en este caso (como vendedor en contacto con el público), podemos considerar que las tareas encomendadas al trabajador implicaban la restricción de su derecho a permanecer en el anonimato de tal suerte que pudiera entenderse que era la propia voluntad del trabajador –expresada al celebrar el contrato– la que*

3.2. Tratamiento de datos sanitarios en la relación de trabajo.

Una vez abordada las cuestiones relacionadas con el tratamiento de datos generales que puede realizar el empresario es el momento de tratar algunas peculiaridades en relación con el procesamiento de datos médicos en las relaciones laborales. Siguiendo la ordenación realizada sobre los datos de salud en función de su mayor o menor repercusión en el desarrollo de la relación de trabajo, hay que precisar en cada caso lo relativo a las exigencias que se derivan, en términos de garantías para los trabajadores, de lo establecido en la LOPD (y expresado en sus principios básicos) en cuanto al procesamiento de informaciones referidas a la vigilancia de la salud.

Así, y teniendo en cuenta el principio de calidad, debe quedar demostrado que el interés empresarial en el conocimiento de esos datos obtenidos de los reconocimientos médicos tiene como única finalidad el realizar una correcta política preventiva en la empresa[719]; y para efectuar un control sobre el absentismo laboral como consecuencia del padecimiento en algún momento de la relación de trabajo de alguna dolencia física o psíquica que le pueda hacer ausentarse de su puesto de trabajo. Así pues, cualquier uso incompatible con estos objetivos iría en contra del principio de calidad, ya que

---

legitimaba la misma, pues es claro que existen actividades que traen consigo, con una relación de conexión necesaria, una restricción en tal derecho por su propia naturaleza, como son las actividades en contacto con el público o accesibles a él, por lo que no puede entenderse que quebranta el derecho a la intimidad de la persona, dar a conocer la identidad del trabajador, cuando queda dentro del triple ámbito de la actividad de venta que abarca a empresa-trabajador-cliente, cuando ello por sí solo no conlleva los datos necesarios para acceder a informaciones relativas directamente a su vida íntima, personal y familiar".

[719] Art. 14.2 de la LPRL: "*En cumplimiento del deber de protección, el empresario deberá garantizar la seguridad y la salud de los trabajadores a su servicio en todos los aspectos relacionados con el trabajo. A estos efectos, en el marco de sus responsabilidades, el empresario realizará la prevención de los riesgos laborales mediante la integración de la actividad preventiva en la empresa y la adopción de cuantas medidas sean necesarias para la protección de la seguridad y la salud de los trabajadores, con las especialidades que se recogen en los artículos siguientes en materia de plan de prevención de riesgos laborales, evaluación de riesgos, información, consulta y participación y formación de los trabajadores, actuación en casos de emergencia y de riesgo grave e inminente, vigilancia de la salud, y mediante la constitución de una organización y de los medios necesarios en los términos establecidos en el capítulo IV de esta ley. El empresario desarrollará una acción permanente de seguimiento de la actividad preventiva con el fin de perfeccionar de manera continua las actividades de identificación, evaluación y control de los riesgos que no se hayan podido evitar y los niveles de protección existentes y dispondrá lo necesario para la adaptación de las medidas de prevención señaladas en el párrafo anterior a las modificaciones que puedan experimentar las circunstancias que incidan en la realización del trabajo".*

no quedaría justificada la intervención del empresario ni el registro de esa información de los trabajadores. En todo caso, y aun siendo el expresado el propósito principal del tratamiento de datos, hay que recordar que el empresario tan sólo puede tratar y mantener un registro con los datos referidos a las conclusiones de esos controles de salud, ya que para realizar las acciones preventivas en su empresa y de adecuación de puestos de trabajo tan sólo necesita conocer esos datos[720].

No obstante, el empresario es el que contrata la realización de esos reconocimientos médicos por lo que, aunque el acceso y tratamiento de los datos se limite sólo a las conclusiones realmente este empresario es el que delega la realización de los exámenes médicos a otras empresas. De todas formas, esta relación entre la empresa que realiza las pruebas médicas a los trabajadores y el empresario es una prestación de servicios determinada, la cual no habilita al empresario a conocer otras informaciones que vayan más allá de la organización preventiva de su empresa, es decir, los resultados de los reconocimientos médicos serán conocidos y archivados por el personal médico que los realiza, sin que puedan trascender a otros sujetos que no tengan esta catalogación dentro de la empresa.

En cuanto al registro de situaciones de incapacidad laboral, el principio de calidad se respeta en cuanto que es obvio y legítimo el interés y la necesidad por parte del empresario de estar al corriente de las bajas por incapacidad temporal en la empresa y, por consiguiente, de llevar un control de las mismas a través de la creación de un fichero con esa información. Sin embargo, el alcance de la protección de los datos personales del trabajador hace que la información a la que pueda tratar el empresario sea mínima ya que no está facultado para registrar en sus bases de datos ningún dato acerca del diagnóstico médico del trabajador[721], puesto que este es irrelevante para la finalidad que pretende el empresario que es la organización de los recursos humanos de la empresa. Ciertamente, con estos datos no se puede llegar a tener mucho conocimiento sobre el estado de salud de los trabajadores, por lo

[720] Vid. apartado 4.1 del presente Capítulo.
[721] Art. 1.2 del RD 575/1997.

que es claro que la finalidad de su tratamiento tenga objetivos encaminados a por un lado, velar por la vigilancia de la salud de los trabajadores; por otro, conocer las posibles bajas laborales para poder establecer alguna sustitución de los trabajadores durante el tiempo que dure la incapacidad[722]; y, finalmente, a efectos de la Seguridad Social, para establecer sus obligaciones y cargas en cuanto a las situaciones de incapacidad temporal[723].

Respecto del tratamiento de datos sobre el código genético de los trabajadores hay que precisar que el empresario lo que pretende con esta acción es certificar la idoneidad de ese empleado en el momento de entrada en la empresa y durante el desarrollo de su relación de trabajo[724]. Por este motivo, el tratamiento de estos datos por el empresario no puede ir más allá de la comprobación de dicha idoneidad para desempeñar el puesto de trabajo con diligencia, no admitiéndose la realización de estos test genéticos para pronosticar que en el futuro ese trabajador va a contraer una determinada enfermedad o patología que no le permita ejercer su actividad, ya que esa información vulnera todos los cánones constitucionales relativos a la ponderación de los intereses en conflicto al tratarse de una medida que no respeta los principios de pertinencia, necesidad, idoneidad y proporcionalidad exigidos por una constante jurisprudencia constitucional.

Podría ocurrir, no obstante, que las condiciones de trabajo del puesto, de la empresa o del sector de actividad en el que el trabajador desarrolle su tarea, pongan en peligro la salud del propio trabajador por estar, por ejemplo, en contacto con algunas sustancias que puedan provocar en el futuro el desarrollo de alguna patología. Sólo entonces quedaría justificado el registro de esas

[722] LÓPEZ INSUA, B.M.: "El control del uso correcto del subsidio por incapacidad temporal: los supuestos de pérdida o suspensión", *Revista Trabajo y Seguridad Social (CEF)*, núm. 394, 2015, pág.109.

[723] Acerca del control del estado de salud de los trabajadores y los distintos sujetos que intervienen en el mismo vid., Rodríguez Escanciano, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, Tirant lo Blanch, 2015, pp.193-207.

[724] Sobre los datos genéticos en las relaciones de trabajo, vid., CARDONA RUBERT, M.B.: *Datos sanitarios*…, op. cit., pp. 55-59; FERIA BASILIO, I.: *La tutela del patrimonio genético del trabajador*, Bomarzo, 2013, pp. 240-243; CALVO GALLEGO, F.J.: "Test genéticos y vigilancia de la salud del trabajador", *Derecho y conocimiento*, núm. 2, 2002, pág.7; GOÑI SEÍN, J.L.: "Vigilancia de la salud versus protección de la intimidad del trabajador", en HORTAL IBARRA, J.C*.: Protección penal de los derechos de los trabajadores,* Edisofer, 2009, pág.59.

informaciones para, de esta forma, poder acreditar algún estudio genético con la intención de acreditar la capacidad de ese trabajador para realizar este tipo de trabajo, bajo estas condiciones, sin que en el futuro se vea afectado su estado de salud. Una vez más el empresario tan sólo conocería y podría almacenar aquella información relacionada con la aptitud de ese trabajador para efectuar el trabajo, sin que pueda tratar los datos médicos obtenidos con la realización del examen genético realizado, cuyo fichero estaría en el centro médico habilitado para la realización de dichas pruebas.

Sobre este asunto, hay que precisar que la singularidad de los tests genéticos no permite que se archiven sólo las especificaciones de los riesgos inherentes a los puestos de trabajo, dando resultados globales que van más allá del objetivo propuesto que es la verificación de su capacidad para desarrollar un puesto de trabajo concreto, por lo que no se estaría cumpliendo el principio de calidad si se tratan más datos de los necesarios para averiguar esta circunstancia, convirtiendo al trabajador en un sujeto totalmente transparente en cuanto a su información personal. De ahí, que no se pueda considerar un medio lícito por cuanto no permite minimizar la recogida de datos limitándola a la finalidad perseguida, por lo que estos test se presentan como un mecanismo subsidiario que sólo podrá realizarse cuando no exista otro que certifique la idoneidad del trabajador[725]

Lo mismo ocurre cuando el empresario ordena realizar, a los servicios médicos que colaboran con su empresa y se encargan de su política preventiva, un test de alcohol o drogas a los trabajadores de su empresa, cuya actividad pueda verse bastante perjudicada por el consumo de estas sustancias[726]. Es decir, en el desarrollo de la relación laboral se admite el tratamiento de estos datos sólo para confirmar la aptitud del trabajador para ese concreto puesto de trabajo, teniendo en cuenta que el empresario lo único que pretende es preservar su organización productiva y la buena marcha de su

[725] GOÑI SEÍN, J.L.: "Análisis genéticos en el ámbito laboral", *Revista de Derecho Social*, núm. 47, 2009, pp. 84-87.
[726] La realización de estos tests sigue el mismo esquema que lo ya tratado en el apartado 4.1 del Capítulo segundo.

empresa[727]. Por tanto, el empresario no podrá registrar más información de la realmente necesaria para constatar la diligencia de ese trabajador a la hora de realizar la prestación de servicios encomendada, ni podrá pedir a los servicios médicos la averiguación de otras informaciones complementarias al propio reconocimiento médico que le permitan archivar datos no relacionados con ese cometido.

Ahora bien, puede ocurrir que el empresario estime que a un concreto trabajador se le hagan esos tests como consecuencia de la existencia de una sospecha fehaciente que le pueda hacer pensar que ese trabajador acude a trabajar presentando anomalías o trastornos derivados del consumo de alcohol o drogas[728], siendo en este caso el examen necesario no sólo para el buen funcionamiento de su trabajo, sino también para no provocar problemas en el desarrollo de la relación laboral y un clima perjudicial para el resto de trabajadores de la empresa. Pero, en estos casos tampoco podrá tratar más datos de los relacionados con la verificación de su capacidad para efectuar el trabajo, ya que si se almacenaran más datos sin que el objetivo fuera la correcta gestión del personal de la empresa si se estaría atentando contra el principio de calidad[729].

En todo caso, el principio de calidad también determina que la recogida de cualquier dato, entre los que se encuentran los sanitarios, tiene que realizarse por cualquier medio lícito, quedando prohibido el recurso a vías de obtención de información que no tengan la legitimidad suficiente y que puedan ser consideradas fraudulentas[730]. Si estas informaciones llegaran a tramitarse y

[727] CARDONA RUBERT, M.B.: *Datos sanitarios*…, op. cit., pp. 61-63.
[728] Sobre la sospecha o posibilidad de realizar pruebas que certifiquen el consumo del alcohol y drogas de los trabajadores vid., art. 2.2.5 y 7 de la OIT: *Tratamiento de cuestiones relacionadas con el alcohol y las drogas en el lugar de trabajo.* Repertorio de recomendaciones prácticas de la OIT, Ginebra, 1996, disponible en http://www.ilo.org/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/normativeinstrument/wcms_112634.pdf [Consulta 25/11/2015]
[729] Véase el documento acerca de los "Principios rectores para pruebas destinadas a detectar el consumo de alcohol y de drogas en el lugar de trabajo adoptados por la reunión interregional tripartita de expertos de la OIT celebrada del 10 al 14 de mayo de 1993 en Oslo (Honefoss), Noruega, disponible en http://www.pnsd.msssi.gob.es/pnsd/legislacion/pdfestatal/i93.pdf [Consulta 25/01/2016].
[730] Art. 4.7 de la LOPD: *"Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos".*

archivarse por algún medio no considerado legítimo[731] y, sobre todo, llegaran a ser tratadas por personal no autorizado, como el empresario, se podría perjudicar a ese trabajador, ya que éste no tiene conocimiento de que se ésta creando un fichero distinto al que manejan los responsables sanitarios, cuyo responsable ahora es el propio empleador. Puede ocurrir que el empresario realice estas averiguaciones ilícitas bajo la existencia de alguna sospecha que le haga reflexionar acerca de las dificultades médicas de ese trabajador, pero lógicamente la forma de investigar estos datos no es la más adecuada. El empresario podría solventar esta situación sometiendo a ese trabajador a un nuevo examen médico más específico que le revelará su capacidad para llevar a cabo la tarea encomendada, pudiendo ser relevado por otro trabajador si no tuviera la aptitud recomendada.

Una vez más, hay que contrastar las exigencias de protección y de garantías que se derivan del *principio de información,* tan esencial como el de calidad en el tratamiento de los datos de salud de los trabajadores. Siendo la finalidad de este principio la de asegurar que el trabajador esté plena y adecuadamente informado de los distintos tratamientos de datos a los que va a estar sometida su información médica. En este sentido, el trabajador tiene que conocer si se ha creado un fichero que contenga sus datos de salud y, a su vez, qué entidades o personas van a ser titulares de ese fichero frente a las cuales, en cuanto responsables, podrá ejercer[732], si así lo decide, sus derechos de acceso, cancelación, rectificación y oposición. Esto, sin olvidar, el derecho que tiene el trabajador a ser informado por parte del responsable del fichero de las posibles cesiones o comunicaciones de sus datos médicos que pudieran darse en el marco de su relación laboral[733].

---

[731] El empresario actuaría en contra de lo establecido en el art. 4.7 de la LOPD si, por ejemplo, pretendiera averiguar datos relacionados con la salud ejerciendo presiones a los responsables sanitarios para que le dieran más información de la que está facultado a conocer; la escucha de conversaciones privadas; rastreo del perfil del ordenador de empresa utilizado por el trabajador para averiguar, si le han enviado por esta vía los resultados de los exámenes médicos, etc.

[732] Vid., apartado Obligaciones y responsabilidades del empresario (4), del presente Capítulo, en el que se establecen los distintos sujetos responsables de los ficheros y las limitaciones que tienen a la hora de constituirlos.

[733] Vid., apartado 5.3 del presente Capítulo.

Una vez ofrecida la información pertinente, el trabajador, en virtud del principio de consentimiento, tiene que otorgarlo para que los datos relacionados con su salud sean tratados. Ciertamente, el consentimiento para tratar las informaciones recogidas por los profesionales sanitarios y otros sujetos facultados para registrar esos datos debe ser expreso[734], pero, a su vez, la LOPD establece algunas excepciones a la exigencia de conformidad del titular del dato. Como, por ejemplo, si el tratamiento de datos vinculados a los resultados de los reconocimientos médicos resulta necesario para la prevención o diagnóstico médico; para las prestaciones sanitarias; o para la realización de actuaciones relacionadas con la protección del interés vital, en este caso, de los trabajadores, tal y como establece el art. 7.6 de la LOPD[735], que permite excluir la necesidad del consentimiento del trabajador si ese procesamiento de datos resulta ineludible para la prevención o diagnóstico médico; para las prestaciones sanitarias; o para la realización de actuaciones relacionadas con la protección del interés vital, en este caso, de los trabajadores. Por ello, si se diera alguna de estas situaciones estos profesionales médicos podrían tratar los datos con esta finalidad sin precisar el consentimiento del titular de esas informaciones pero, en estos casos, tampoco el empresario podría tratar esos datos médicos ya que su registro y control no se encuentra bajo su sistema de organización, como ya se ha comentado[736].

Si los datos de que se trata se refieren sólo a las conclusiones, relacionadas con la aptitud para desarrollar el trabajo, a las que puede acceder

[734] Ahora bien, para el tratamiento de datos genéticos y debido a la especial relevancia que tiene la averiguación y el tratamiento de estos datos hay algunos autores que han considerado que, además este consentimiento se preste por escrito. Véase: SEONE RODRÍGUEZ, J.A.: "De la intimidad genética al derecho a la protección de datos genéticos. La protección ius fundamental de los datos genéticos en el Derecho español (A propósito de las SSTC 290/2000 y 292/200, de 30 de noviembre)", *Revista de Derecho y Genoma Humano*, núm. 17, 2002, pág. 158.

[735] Art. 7.6 de la LOPD: *"No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento".*

[736] Vid, distinción entre la obtención de resultados y conclusiones, y las personas encargadas de su conocimiento, apartado 2.2 del presente Capítulo.

el empresario, la LPRL, como se ha dicho, faculta al empresario y a los órganos con responsabilidad preventiva[737] a acceder a esas conclusiones, con el objetivo de que *"puedan desarrollar sus funciones de forma correcta",* por lo que no es necesario consentimiento alguno del trabajador. Con estas conclusiones[738] no se valora la enfermedad que pueda tener el trabajador, sino su aptitud para el desarrollo de un determinado puesto de trabajo, independientemente de la situación médica que tenga el trabajador pues puede ser apto para un trabajo concreto y no apto para otro en el que se le exigiera unas determinadas condiciones físicas que no cumpliera. Por ejemplo, para ejercer la profesión de bombero se requieren unas cualidades físicas y psíquicas que si un trabajador no las tiene no significa que no pueda dedicarse a otra profesión para la cual podría estar perfectamente cualificado[739].

Tampoco constituye un tratamiento de datos médicos el registro de las conclusiones cuando éstas se refieren a datos generales que no vinculan a ningún trabajador concreto, distintos de aquellos que se refieren a la aptitud o no para ejercer la prestación de trabajo. Estas informaciones son las almacenadas por el empresario para cumplir la obligación del citado art. 23 de la LPRL – relación de accidentes de trabajo, enfermedades profesionales, planificación de la actividad preventiva etc.-, las cuales no se refieren individualmente a ningún trabajador de la empresa, a menos que como

---

[737] Estos órganos con responsabilidad preventiva quedan definidos en la LPRL y son; Delegados de Prevención, Comité de Seguridad y Salud y la representación unitaria y sindical de los trabajadores, al igual que aquellos trabajadores designados para tareas preventivas.

[738] Art. 22. 4 de la LPRL: *"…No obstante lo anterior, el empresario y las personas u órganos con responsabilidades en materia de prevención serán informados de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva".*

[739] Sentencia del TSJ Andalucía de 6 de abril de 1998 (RJCA 1998\1146); *"Pero al margen de lo expuesto y aun aceptando que una cifra de colesterol superior al máximo permitido pudiera calificarse como una «enfermedad o anomalía endocrino metabólica», no podría considerarse, en el caso concreto que analizamos la existencia de tal enfermedad, a los efectos de declarar la ineptitud física del recurrente, puesto que para que el colesterol pueda considerarse como factor de riesgo cardiovascular, debe detectarse una cifra superior a 250 mg/100 ml, sin que una cifra aislada tenga valor diagnóstico ni pronóstico cuando se encuentra en límites cercanos a la normalidad, máxime si se tiene en cuenta que en los análisis practicados al recurrente posteriormente, se apreció una cifra más baja, por lo tanto, no siendo admisible una interpretación extensiva de las causas de exclusión por indiciaria de futuros riesgos cardio circulatorios que sea la cantidad de colesterol en sangre del actor, lo procedente es la declaración de nulidad de los actos impugnados".*

consecuencia de la dimensión de la empresa se pudiera identificar a un empleado tan sólo con el procesamiento de esas conclusiones.

Por ello, el empresario sólo puede tratar sin consentimiento los datos derivados de las conclusiones, teniendo en cuenta que no constituyen informaciones médicas ni, en ocasiones, pueden llegar a ser identificativas de un trabajador determinado. Cierto es, que las conclusiones que revelan la aptitud de un trabajador si individualizan a ese empleado y sí están catalogadas como dato de carácter personal, aunque no sería necesario solicitar el consentimiento inequívoco para su tratamiento, ya que éste es necesario para el correcto mantenimiento y funcionamiento de la relación de trabajo, en virtud de lo establecido en el art. 6.2 de la LOPD[740].

Cuando los datos acerca de la salud de los trabajadores quieran utilizarse para gestionar el absentismo laboral, es conveniente hacer alguna aclaración referida a la prestación del consentimiento para tratarlos. Como regla general ya se ha dicho que[741], el tratamiento de datos de salud requiere del consentimiento expreso del afectado o de la existencia de una previsión legal que exima del mismo. Esta excepción basada en la existencia de una norma que habilite el tratamiento del dato podría darse en el caso del tratamiento de datos para la gestión del absentismo laboral, siguiendo lo establecido en el art. 20.4 del ET[742], siempre que estos datos para gestionar el absentismo laboral no sean descriptivos o reveladores de circunstancias médicas. No obstante, se ha afirmado que, pese a que la jurisprudencia constitucional haya prohibido la creación de ficheros que contengan información acerca de las bajas laborales de los trabajadores si no ha mediado el consentimiento de ese trabajador para ello[743], la posibilidad de crear y

[740] GOÑISEÍN, J.L.: "Vulneración de los derechos fundamentales en el trabajo…", op. cit., pp. 59-60.
[741] Vid., apartado 4 del Capítulo II.
[742] Art. 20.4 del ET: "El empresario podrá verificar el estado de enfermedad o accidente del trabajador que sea alegado por éste para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones".
[743] Sentencia del Tribunal Constitucional 202/1999, de 8 de noviembre (RTC 1999, 202) ,cuando razona que el fichero está fuera de las excepciones del artículo 7 de la LOPD pues no

mantener ese tipo de fichero de datos se prevé como necesaria para que el empresario pueda realizar un control del absentismo y sólo con ese objetivo, por lo que para ese supuesto se podrá prescindir del consentimiento[744] existiendo habilitación legal que aunque no establezca la anotación de las bajas laborales en sentido estricto le otorga al empresario la facultad de control de las ausencias del centro de trabajo, sin que esto sea posible sin un registro de las mismas[745].

3.3. Libertad sindical y tratamiento de datos.

En ocasiones y por variadas circunstancias, el empresario puede acceder a información sindical referida a sus trabajadores. Con finalidades legítimas como la organización del trabajo (información sobre el uso de horas sindicales, por ejemplo), el cumplimiento de las exigencias legales en materia sindical (permisos para negociación, crédito de horas y su posible acumulación, permisos formativos, prerrogativas de los delegados sindicales y de las uniones sindicales de empresa), la adopción de medidas en el contexto de un conflicto colectivo (descuento de horas por huelga, situación de alta especial en la Seguridad Social, prestación de servicios mínimos [746] o de mantenimiento), o en cumplimiento de los acuerdos colectivos que le obligan a realizar en la nómina de los trabajadores, de forma individualizada, el descuento del canon

---

se dirige a la preservación de la salud de los trabajadores, sino al control del absentismo laboral; por lo que la existencia del mismo sin el consentimiento expreso del afectado es una medida inadecuada y lesiona el derecho de libertad informática. Por lo demás no es de aplicación el artículo 8 de la LOPD, pues dicha norma que regula la cesión de datos relativos a la salud de las personas, parte de la previa existencia de un fichero legal de datos, y ya hemos visto que este no es el caso. En el mismo sentido vid., Sentencias de la Audiencia Nacional de 12 de abril (PROV 2002, 143466) y 10 de mayo de 2002 (PROV 2003, 49667).

[744] Sobre este aspecto vid., la interesante reflexión realizada por RODRÍGUEZ ESCANCIANO, S. acerca de la posibilidad de tratar los datos de absentismo laboral sin el consentimiento de los trabajadores en su libro *Poder de control empresarial, sistemas tecnológicos…,* op.cit., pp.208-211.

[745] Art. 54.2 a) del ET: *"Se considerarán incumplimientos contractuales: a) Las faltas repetidas e injustificadas de asistencia o puntualidad al trabajo".*

[746] Art. 6.7 del Real Decreto Ley 17/1977, de 4 de marzo, sobre las relaciones de trabajo (BOE núm. de 9 de marzo de 1977): "*El comité de huelga habrá de garantizar durante la misma la prestación de los servicios necesarios para la seguridad de las personas y de las cosas, mantenimiento de los locales, maquinaria, instalaciones, materias primas y cualquier otra atención que fuese precisa para la ulterior reanudación de las tareas de la empresa. Corresponde al empresario la designación de los trabajadores que deban efectuar dichos servicios.*

sindical), el empresario puede hacer uso de los datos sobre la afiliación sindical de los empleados[747].

Sin embargo, el tratamiento por parte del empresario de estos datos debe ir encaminado a cumplir los objetivos estrictos para los que los ficheros se crean (principio de calidad), es decir, que se utilicen para las finalidades anteriormente descritas, sin que el tratamiento de datos relacionados con la afiliación sindical persiga otros propósitos que puedan perjudicar al trabajador. Pudiera ocurrir que el almacenamiento de estos datos pretendiera, por ejemplo, descontar el día de huelga a los trabajadores afiliados al sindicato, independientemente de que éstos hubieran secundado la huelga o no, provocando un perjuicio a aquellos trabajadores que no han participado en la misma; o que el empresario decidiera crear un fichero con datos relacionados con la afiliación sindical para controlar a esos trabajadores de forma más pormenorizada, teniendo en cuenta sus inquietudes sindicales[748]. Si se crearan estos archivos, evidentemente, no se estaría cumpliendo con el principio de calidad, ya que parece ser que el empresario estaría persiguiendo otros objetivos distintos y no permitidos con el registro de esos datos.

Además, en virtud de los principios de información y de consentimiento, para la utilización de estos datos dentro del marco organizativo empresarial, será preciso que se informe al trabajador sobre el sentido y la finalidad del archivo de este dato especialmente sensible y que concurra su consentimiento expreso y por escrito ya que no existe ninguna excepción en la LOPD que permita el tratamiento de estos datos relacionados con el ejercicio de la actividad sindical sin que se tenga la conformidad del trabajador afectado.

Ahora bien, aunque no se trata propiamente del empresario, procede hacer algunas reflexiones acerca de la protección que de ese dato personal de

[747] Vid. apartado 2.2. del presente Capítulo.
[748] DÍAZ RODRÍGUEZ, J.M.: "Intimidad y privacidad sindical frente al control empresarial" *Comunicación presentada al XXIV Congreso nacional de Derecho del Trabajo y Seguridad Social*, Pamplona, 2014, pág.7; DAVARA RODRÍGUEZ, M.A.: "La relación entre los artículos 28.1 CE (Libertad sindical) y 18.4 CE (tratamiento automatizado de datos de carácter personal), desde la óptica de la llamada "protección de datos personales", *Repertorio Aranzadi del Tribunal Constitucional,* vol. IV, parte Estudio, 1998, pp. 7-9.

la afiliación (y otros asociados a ella, también de carácter personal) den el ámbito de la propia organización sindical[749], los cuáles deben cumplir también las premisas marcadas por la LOPD.

Al igual que ocurre con todos los ficheros de datos de carácter personal estas bases de datos tienen que atender a las finalidades recogidas en el inicio de la relación sindical entre trabajador y sindicato, es decir, el tratamiento que el sindicato pueda cometer para con los datos de sus afiliados será pertinente y adecuado a las actividades relacionadas con la afiliación sindical. Puede ocurrir que se pueda infringir ese principio si se realizan reclamaciones ante la empresa que no siempre son conocidas ni consentidas por los trabajadores, ejerciendo sus funciones de garantes o protectores de los derechos de los trabajadores. En este sentido, se podría estar atentando con el principio de racionalidad o pertinencia de los datos, ya que los datos obrantes en los ficheros sindicales se estarían utilizando para finalidades no compatibles, por ejemplo, si el sindicato se dirige a la empresa, cuyos datos le ha facilitado el propio afiliado, para exigir el cumplimiento de algún derecho que no ha sido reclamado por parte de ese asociado.

Cuando se tratan datos relacionados con la afiliación sindical lo habitual es que se solicite el consentimiento expreso y por escrito del trabajador, pero cuando son ficheros cuya propiedad pertenece a los sindicatos la LOPD establece una excepción específica para este registro de información, prescindiendo del citado consentimiento cuando la organización sindical necesite almacenar esos datos para efectuar sus funciones[750]. Esta excepción al consentimiento no excluye el derecho que tiene el trabajador a estar debidamente informado sobre las actividades del sindicato y sobre el uso que

[749] La información necesaria para afiliarse a un sindicato es la referida a: datos identificativos; datos profesionales; situación laboral; número de cuenta bancaria; y los datos de la empresa dónde realiza su actividad laboral el afiliado.

[750] Art. 7.2 de la LOPD: *"Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado."*

se le va a dar a los datos recogidos por el mismo, pudiéndose negar a que se traten los datos si no está de acuerdo con sus distintos usos[751]. Ahora bien, la LOPD[752] establece que se podrá soslayar este derecho a la información de los trabajadores, cuando la transmisión de la información sobre la utilización de los datos de los trabajadores se realice con el único objetivo, por ejemplo, de poner en marcha la actividad sindical del organismo y que el traslado de la información conlleve esfuerzos desproporcionados, como consecuencia del elevado número de trabajadores afiliados a la organización sindical.

4. OBLIGACIONES Y RESPONSABILIDADES DEL EMPRESARIO RELACIONADOS CON EL CUMPLIMIENTO DE LA LOPD.

4.1. Obligaciones del empresario respecto a los datos almacenados en los ficheros empresariales.

La importancia e indispensabilidad que supone para la empresa el tratamiento de los datos personales y profesionales de los trabajadores, no evita la obligación empresarial de respetar en la obtención y, sobre todo en lo que aquí interesa, en el tratamiento de datos las exigencias de la normativa sobre protección de datos de carácter personal[753], siendo su primera obligación

[751] RODRÍGUEZ ESCANCIANO, S.: "El derecho a la protección de datos personales de los trabajadores como garantía de la libertad sindical" *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 27, 2011, pp. 71-73; TAPIA HERMIDA, A.: "Uso del correo electrónico para transmitir información de naturaleza laboral y sindical a los trabajadores, por las organizaciones sindicales, en los centros de trabajo y durante la jornada laboral", *Revista de Trabajo y Seguridad Social* CEF), núm. 276, 2006, pp. 141 y ss; ALZAGA RUIZ, I.: "El uso por parte de la representación sindical de los medios informáticos propiedad de la empresa (Comentario a la Sentencia del Tribunal Constitucional 281/2005, de 7 de noviembre)", *Revista Española de Derecho del Trabajo*, núm. 132, 2006, pp. 1047 y ss.

[752] Art. 5.5 de la LOPD: *"No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten".*

[753] DEL REY GUANTER, S.: "Tratamiento automatizado de datos de carácter personal y contrato de trabajo. Una aproximación a la "intimidad informática" del trabajador", *Revista Relaciones Laborales,* núm. 2, 1993, pág. 17; SAGARGOY DE SIMÓN, I.: "Datos personales, datos profesionales y su tratamiento automatizado", *Revista Relaciones Laborales,* núm. 1, 1995, pág. 1456; THIBAULT ARANDA, J.: "La incidencia de la Ley Orgánica 15/1999, de 13 de

la del almacenamiento de esos datos en un fichero, ya sea automatizado o manual[754], con la finalidad de controlarlos de mejor forma y poder acceder a su conocimiento de manera más organizada y precisa. Es, pues, a partir de la existencia de un fichero cuando se puede empezar a hablar de tratamiento de datos.

4.1.1. Justificación, naturaleza y excepciones.

El fichero tiene que ser creado con la justificación de cumplir una serie de objetivos y funciones legítimas desde el punto de vista de la empresa pero que deben quedar precisados, y suficientemente justificada la creación y existencia de un fichero de esa naturaleza. En este sentido, podrían considerarse, siempre que se realizaran de forma más precisa y completa, como objetivos legítimos y respetuosos con la LOPD, la finalidad organizativa del trabajo, la vigilancia y el análisis de las medidas de prevención, la formativa o la financiera de la empresa, la organización funcional y la promoción, etc.[755].

Para la configuración de estos ficheros con datos de trabajadores, y siguiendo lo establecido en la LOPD y en el RDLOPD[756] el empresario tiene

---

diciembre, de protección de datos de carácter personal, en el ámbito de las relaciones laborales*"*, *Revista Relaciones Laborales,* núm. 2, 2000, pág. 34; GARCÍA-NÚÑEZ SERRANO, F.: "La regularización sobre protección de datos personales y su incidencia en el ámbito laboral", *Aranzadi Social*, núm. 5, 2000, pág. 1110.
La normativa sobre protección de datos distingue entre ficheros automatizados o no, siendo los primeros aquellos ficheros organizados en un soporte informático a los que se pueda acceder utilizando cualquier tipo de aplicación informática. En cuanto a los ficheros no automatizados tienen una definición legal en el art. 5.1 d) RDLOPD; *"Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica"*. Como es obvio, en los ficheros automatizados es más sencillo el acceso o la búsqueda de un determinado dato de carácter personal, debido a las ventajas que ofrece la informática, lo que no sucede en los no automatizados donde la búsqueda de algún dato de carácter personal puede suponer un mayor esfuerzo y una menor rentabilidad informativa . En todo caso, ambos quedan bajo la influencia de la normativa de protección de datos. En las empresas dónde, por la dimensión de la plantilla esencialmente, existe un gran volumen de datos, los ficheros que utilizan los empresarios para almacenar datos de los trabajadores suelen estar informatizados, mientras que en las empresas pequeñas el uso de la infraestructura informática se sustituye con frecuencia por la creación de ficheros de datos manuales que, sin embargo, gozan de la misma protección que si formaran parte de un fichero automatizado.

[755] Sobre este aspecto la AEPD en su Informe 156/2008 hace una amplia reflexión sobre los distintos ficheros que pueden configurarse en el ámbito laboral, más concretamente, aquéllos de los que es responsable el empresario.

[756] Arts. 20 y 25 de la LOPD; y arts. 52 y ss. del RDLOPD.

que hacer una distinción entre ficheros de naturaleza pública o privada; calificándose los ficheros empresariales con datos de los trabajadores como de naturaleza privada[757], puesto que la persona encargada de gestionar el fichero tiene esa naturaleza[758]. No obstante, hay que tener en cuenta que la variedad de relaciones de trabajo, Por ejemplo, aquellos trabajadores que ejerzan su actividad dentro de las entidades públicas empresariales, puede configurar otros ficheros que revistan naturaleza pública, los cuales tienen unos requisitos para su creación distintos de los de naturaleza privada como se verá cuando se analicen los ficheros creados en el marco de la Administración Pública[759].

Pese al sometimiento general de los ficheros de datos personales del trabajador a la normativa sobre protección de datos, el empresario puede recoger algunos datos identificativos[760] de los trabajadores sin que éstos queden sometidos a las exigencias de la LOPD al considerarse que se trata de informaciones, aunque referidas a la persona del trabajador, excluidas de su ámbito de aplicación. Acerca de la ausencia de protección para los datos identificativos y relacionados con su puesto de trabajo de los trabajadores la AEPD ha establecido la validez de este criterio en el que se elimina la protección de determinados datos de los trabajadores. Esta interpretación, de la AEPD, es imprecisa pues no parece aceptable que esos datos se encuentren desprotegidos respecto a la utilización que pueda hacer el empresario de los

[757] Art. 25 de la LOPD: *"Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas".*

[758] VV.AA: "Una aproximación para empresas a la Ley Orgánica de Protección de Datos", *Derecom*, núm.15, 2013, pp. 96-97; NAVALPOTRO NAVALPOTRO, Y.; "Ámbito de aplicación de la Ley Orgánica de protección de datos de carácter personal (LOPD)" en VV.AA. *Estudio práctico sobre la protección de datos de carácter personal*, Lex Nova, 2005, pp. 58-60. SANTOS GARCÍA, D.: *Nociones generales de…,* op. cit., pág.43.

[759] Vid., apartado 5.1.2 del presente capítulo.

[760] Art. 2.2. del RDLOPD: *"Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales*".

citados datos de carácter personal, tratándose por consiguiente de una exención desproporcionada[761].

Se trata de los datos expuestos en las denominadas listas profesionales (nombre, apellidos, funciones o puestos desempeñados, dirección postal o electrónica, teléfono y número de fax profesionales). Una excepción que puede favorecer un uso en exceso flexible por parte del empresario de tales datos en cuanto a todo lo relacionado con la gestión del personal, por lo que podría haberse hecho de otra forma, estableciendo otros requisitos para su tratamiento que no implicaran la desprotección total de esa información. La diferenciación d estas informaciones en otros ficheros se hace cuanto más complicada, ya que para la correcta gestión de los recursos humanos de la empresa es necesario que esas informaciones se vaya completando con otras para cuyo tratamiento si se requiere el cumplimiento de los principios de la LOPD, por ejemplo el nombre y apellidos del trabajador va estar unido con su cualificación profesional, datos retributivos, su DNI, número de afiliación a la Seguridad Social etc.[762].

4.1.2. Tipos de ficheros e inscripción.

Además de la inclusión de los datos en un fichero el empresario está obligado a catalogar las distintas tipologías de datos que maneja, estableciendo una ordenación sistemática de los mismos. Es decir, si el empresario recoge datos que requieran una especial protección, éstos tendrán que permanecer en otros ficheros pues, como ya se ha visto[763], para el tratamiento de estos particulares datos la norma exige una serie de requisitos específicos.

Es el caso de los ficheros que contengan datos sensibles de los trabajadores respecto de los cuales el empresario está obligado a respetar la

[761] Informe de la AEPD 42/2008, disponible en http://www.agpd.es/portalwebAGPD /canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2008-0042_Novedades-del-Reglamento-respecto-a-empresarios-individuales.pdf[Consulta 22/09/2014].
[762] GUALDA ALCALÁ, F.J.: "La protección de datos personales…", op. cit., pp. 263-265; VILASAU SOLANA, M.: "El fin de la situación de transitoriedad: la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal ya tiene desarrollo reglamentario", *Revista de Internet, Derecho y Política (UOC)*, núm. 7, 2008, pág.5.
[763] Vid. apartado 3.1 y 3.2 del presente Capítulo.

prohibición de la LOPD de crear ficheros con la finalidad exclusiva de almacenar datos referidos a la salud y a la afiliación sindical, entre otros datos de carácter personal e íntimo[764], salvo la excepción de las entidades encargada de tratar datos relacionados con la salud de los trabajadores den relación con las medidas de prevención; o de los ficheros sindicales creados para el mejor cumplimiento sindical de sus obligaciones y compromisos con los sindicatos y con la representación de los trabajadores; o cuando así se disponga legislativamente[765].

Además, el empresario debe, en su condición de titular del fichero de datos de carácter personal, inscribirlo ante la AEPD[766], en virtud del procedimiento establecido en el art. 26 de la LOPD[767]. Un requisito que, cumplido formalmente[768], sigue siendo hoy más una técnica evasiva[769] encaminada a evitar una posible sanción. Lo que suele llevar a la inscripción de

[764] Art. 7.4. de la LOPD: *"Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual".*

[765] Art. 14.2 de la Ley 41/2002 de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica,: *"Cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información".*

[766] Sobre este aspecto véase apartado 4.2 del Capítulo I.

[767] Art. 26 de la LOPD: *"1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos. 2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros. 3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación. 4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación. 5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos".*

[768] La inscripción de ficheros de titularidad privada total en el año 2014 es de 3.594.106. Habiendo experimentado, desde el año 2008-2010 un incremento anual en la inscripción de ficheros y disminuyendo esas inscripciones del año 2010 hasta el 2014. Fuente: Memoria de la Agencia Española de Protección de Datos de Carácter Personal, 2014, pág. 131.

[769] HERBERT, A.S.: "What computers mean form and society", en VV.AA. *Microelectronics revolutions*, Forrester. T. ed, pp. 123 y ss; VALVERDE ASENCIO, A.J. "El derecho a la protección de datos en la relación laboral" en VV.AA *Relaciones Laborales y Nuevas Tecnologías*, La Ley 2005, pp. 384-385; BUSTO LAGO, J.M.: "La Responsabilidad Civil de los responsables de ficheros de datos personales y de los encargados de su tratamiento", *Revista Doctrinal Aranzadi Civil-Mercantil,* núm. 5, 2006, pp. 3-5.

ficheros poco precisos y nada descriptivos de los datos que realmente se tratan.

4.1.3. Medidas derivadas del principio de seguridad y conservación de ficheros.

Una vez que los datos están contenidos en los ficheros, el empresario está obligado, a cumplir con los requerimientos establecidos en la normativa sobre protección de datos, relacionados con la observación de los principios de calidad, información y consentimiento[770]; y con la adopción de las pertinentes medidas de seguridad dependiendo de la naturaleza que tengan los datos allí almacenados. Por este motivo, el empresario tendrá que implantar las medidas técnicas y organizativas necesarias para proteger los datos de carácter personal. Obligado por el principio de seguridad que, como regla general, exige que el responsable del fichero o encargado del tratamiento[771] conozca los riesgos existentes y las medidas de seguridad que pueden establecerse al efecto[772].

De forma general, con la protección basada en las medidas de seguridad lo que se pretende es, de un lado, preservar el derecho a la protección de datos del trabajador ante cualquier acceso no autorizado, independientemente de que ese fichero sea automatizado o no y, también, garantizar el respeto del principio de confidencialidad por parte de los sujetos que van a intervenir en el procesamiento de datos[773]. Consecuentemente con lo anterior, se establece la obligatoriedad de que se incluyan las limitaciones

[770] Sobre la aplicación de estos principios al tratamiento de datos necesarios para la gestión de personal vid., apartado 3 del presente Capítulo.

[771] En el ámbito empresarial y en lo que a la gestión de datos de carácter personales de los trabajadores se refiere la figura del encargado de tratamiento aparece cuando el empresario decide contratar los servicios de una empresa externa para la administración de su personal. En estos casos el empresario cede toda la información que tiene de estos trabajadores a esta empresa externa que inicia con ellos una relación profesional basada en las instrucciones dadas por ellos. La identificación de estas figuras será abordado cuando se traten las cesiones de datos en las relaciones de trabajo, concretamente en el apartado de cesiones a otras entidades (vid., apartado 5.3).

[772] VV.AA.: *Principios y derechos de protección….*op. cit., pág. 547.

[773] MARTIN PARDO DE VERA, M.: "Principios de la protección de datos: seguridad de los datos. Aplicación de los niveles de seguridad (1ª y 2ª parte)", en VV.AA.: *Comentario a la Ley Orgánica de protección de datos de carácter personal*, Civitas, 2010, pp.782-786; FALCÓN Y TELLA, F.: "Medidas de seguridad aplicables a ficheros y tratamientos de datos de carácter personal", *Foro Nueva Época*, núm.8, 2008, pp.196-200.

de acceso en el documento de seguridad[774], creado por el responsable del fichero o encargado del tratamiento con la finalidad de proteger los datos de carácter personal[775]. En cuanto a los niveles de seguridad (básico, medio y alto) es necesario atender la naturaleza de los datos contenidos en los ficheros. Sin embargo, en los ficheros de datos creados por el empresario lo habitual es aplicar las medidas de seguridad de nivel básico[776], que son aquellas que tienen que tener todos los ficheros. Ello con independencia de que, como consecuencia de la gestión de alguno de los datos especialmente protegidos[777], se hiciera necesario exigir medidas de seguridad correspondientes a los niveles medio y alto[778].

La interposición de estas medidas, que aseguran la salvaguarda de la información personal contenida en los ficheros empresariales, tiene distintos rangos. Es decir, si el fichero es automatizado y se encuentra en un soporte informático, para acceder a él será necesario un usuario y contraseña o, incluso, la lectura de una tarjeta de identificación en la que esté incorporado un microchip que identifique claramente a la persona que va a acceder al fichero.

---

[774] Sobre las características del documento de seguridad, véase pág. 94 y ss. .
[775] Vid., art. 88 del RDLOPD.
[776] Art. 81.1 del RDLOPD: *"Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico".*
[777] Así lo expone el Tribunal Supremo (Sala de lo Contencioso-Administrativo) en su sentencia de 13 de marzo de 2012 (RJ 2012\4917); *"El motivo no puede ser acogido, pues sencillamente el principio de igualdad en la aplicación de la ley no es la razón de decidir del recurso contencioso administrativo, sino que al contrario, la Sala de instancia aprecia y tiene en cuenta la falta de identidad entre el supuesto de hecho que enjuiciaba y el caso precedente. En el caso precedente, iniciado por una denuncia de una médico del SESPA, la información recabada por la AEPD no apreció la existencia de ningún incumplimiento en materia de medidas de seguridad en los ficheros de datos de salud, mientras que en el presente caso, la investigación del SESPA fue más amplia, pues incluyó una visita de inspección al Centro de Salud Parque-Somió, con los resultados ya antes explicados de comprobación de una utilización de las historias clínicas mayoritaria y casi exclusiva por vía informática, con protocolos de actuación y medidas de seguridad que se estimaron correctas para el tipo de ficheros de que se trata, y una utilización residual de las historias clínicas en soporte papel, con falta de constancia de las solicitudes, de la entrega y devolución, lo que la sentencia impugnada incluyó en su narración de hechos probado".*
[778] Art. 81.2 f) del RDLOPD: "*Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal; f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos".* Art. 81.3 a) del RDLOPD: *"Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal: a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual".*

Sin embargo, si el fichero no está automatizado y los datos requieren sólo medidas de seguridad de nivel básico, éstas deberán ubicarse en mecanismos que dificulten su lectura. Si, en cambio, se trata de datos en relación con los cuales se hayan implantado medidas de seguridad de nivel alto tendrán que almacenarse en lugares dónde al acceso esté restringido a usuarios que tengan llave u otro dispositivo equivalente para poder entrar a la zona dónde esté ubicada aquella información sensible del trabajador.

El empresario, con el fin de evitar accesos ilegítimos en las bases de datos de la empresa, tendrá que autorizar a las personas que bajo su responsabilidad puedan acceder a los ficheros, fundamentando este acceso como necesario para el desarrollo de la actividad laboral de los trabajadores autorizados[779]. Estos mecanismos de autenticación vienen descritos en el RDLOPD[780] y tendrán que ser configurados previamente al acceso a las bases de datos de los trabajadores. Así pues, el responsable del fichero tendrá que especificar los distintos perfiles de acceso para cada uno de los ficheros creados, dependiendo de las funciones que tenga que realizar el trabajador acreditado para visualizar las bases de datos con información del resto de

[779] El RGPD obliga al responsable del fichero a comunicar a la autoridad de control en el plazo de 72 horas las violaciones de seguridad de los datos personales, entendiendo por tales la alteración, destrucción, perdida, etc. de aquella información personal que se haya transmitido o tratado de forma distinta a la prevista inicialmente (vid., art. 33). De esta forma se le da a la autoridad de control más funciones de supervisión en el cumplimiento de la legalidad para el procesamiento de datos de carácter personal.

[780] Art. 91 del RDLOPD: "1. *Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. 2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos. 3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. 4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero. 5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio."* Art. 93 del RDLOPD*; "El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. 4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible".*

trabajadores del centro de trabajo[781]. Por ejemplo, aquel trabajador que se dedique a gestionar el pago del salario sólo podrá acceder a los datos precisos del trabajador para abonar la nómina y, por consiguiente, únicamente podrá comunicar datos del trabajador a las entidades autorizadas para gestionar la contribución del mismo a la Seguridad Social y o/a la AEAT-[782].

En otro orden de cosas y vinculado a los ficheros con nóminas de los trabajadores, se pueden producir revelaciones de otras informaciones de los empleados que precisen un nivel de protección más elevado. Este es el caso de aquellos datos relacionados con las circunstancias que permitan al empresario practicar distintas retenciones de IRPF por rendimiento del trabajo, dependiendo de su situación familiar o personal, datos que pueden considerarse especialmente protegidos y que tendrán que estar separados de los datos generales necesarios para gestionar el pago de los salarios al trabajador[783], permitiendo implantar las medidas de seguridad pertinentes según la tipología de la información, -nivel medio o alto-.

A estos efectos, en el RDLOPD se proponen algunas pautas más restrictivas, no sólo para el acceso a los datos contenidos en los ficheros con un nivel de protección más alto, sino también para el funcionamiento del mismo. Así, para intentar preservar el acceso a los datos, los soportes automatizados donde se almacenan deberán estar identificados con sistemas de etiquetado que sólo permitan el acceso a los datos especialmente protegidos a aquellas personas autorizadas previamente para ello. Igualmente se cifrarán los dispositivos portátiles que se encuentren fuera del centro de trabajo y, por tanto, fuera del ámbito de vigilancia del responsable del fichero, siempre que éstos sean compatibles con los sistemas de cifrado establecidos en la empresa[784]. Asimismo, se creará un registro de accesos en el que cada

[781] RIBAGORDA GARNACHO, A.: "La protección de datos personales y la seguridad de la información", *Revista Jurídica de Castilla y León*, núm.16, 2008, pp. 385-386.
[782] Sobre las características y legalidad de estas cesiones se va a realizar un análisis en el apartado 3 del presente Capítulo.
[783] Vid., apartado 3.2 del presente Capítulo.
[784] Art. 101 del RDLOPD: *"1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten*

vez que se intente entrar en el fichero se guardarán los datos del usuario, la fecha, la hora y el fichero al que se accede, así como el tipo de acceso y si éste ha sido autorizado o denegado.

No obstante, cuando se den las premisas exigidas en el RDLOPD[785], se podrá excepcionar el establecimiento de las medidas de seguridad de nivel alto, y sustituirlas por las de nivel básico si, por ejemplo, el tratamiento de los datos relativos a la discapacidad del trabajador no sólo venga autorizado en el convenio colectivo, sino que sea necesario para el cumplimiento de los deberes públicos que tenga la empresa. Ahora bien, es preciso tener en cuenta que la normativa sólo hace referencia a la incorporación en el fichero de datos sobre la discapacidad del trabajador, sin que puedan registrarse otros datos relacionados con la salud del afectado, ya que en este caso sí sería necesario establecer medidas de seguridad de nivel alto[786].

---

la identificación para el resto de personas.2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte. Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos".

[785] Art. 81.6 del RDLOPD: *"También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos."*

[786] En este sentido la AEPD se ha pronunciado estableciendo que: "...*las obligaciones que justifican el tratamiento de los datos son legalmente exigibles del propio Banco de España, por aplicación de lo -dispuesto en los artículos 37.1 de la Constitución y 82.3 del Estatuto de los Trabajadores, por lo que puede considerarse que el tratamiento de dichos datos resulta necesario para el cumplimiento por el consultante de obligaciones legales y, en consecuencia, cabrá considerar aplicable la excepción a la imposición de las medidas de seguridad de nivel alto prevista en el artículo 81.6 del Reglamento de desarrollo de la Ley Orgánica 15/1999.debe recordarse que la excepción prevista en dicho precepto se referirá al tratamiento consistente en "la mera indicación del grado o porcentaje de minusvalía del afectado o de los miembros de su unidad familiar", de modo que, como se indica en el citado informe si se incorporasen otros datos relacionados con la salud del afectado, como las circunstancias específicas que determinan el porcentaje de discapacidad del mismo, no será posible entender aplicable el artículo 81.6 del Reglamento, debiendo implantarse las medidas de seguridad de nivel alto", en* Informe Jurídico 336/2008de la AEPD, disponible enhttp://www.agpd.es/portalwebAGPD/canaldocumentacion/ informes_juridicos/medidas_seguridad/common/pdfs/2008-0336_Aplicaci-oo-n-del-art-ii-culo-81.6 -en-caso-de-tratamiento-de-datos-de-discapacidad-para-el-cumplimiento-de-obligaciones-previs tas-en-convenio-colectivo.pdf [Consulta 23/06/2015].

Finalmente, otra de las obligaciones que debe cumplir el sujeto encargado de gestionar estas bases de datos de trabajadores es la relacionada con la conservación de esa información en los ficheros. En este sentido, la normativa sobre protección de datos establece el deber de conservar estos datos por un periodo de dos años, revisando esta información al menos una vez al mes el registro de esos datos y controlando que el funcionamiento de los registros sea el correcto[787].

4.2. Aspectos generales acerca de las responsabilidades del empresario respecto a los datos almacenados en los ficheros empresariales.

Como regla general la responsabilidad del fichero con datos de los trabajadores la tiene el propio empresario o entidad pública que gestione esa información. Cierto es que, existen ocasiones en las que, dependiendo de la tipología de datos que se almacene, pueden aparecer otros sujetos como responsables de los ficheros, como se verá en el análisis siguiente en relación con las bases de datos especialmente sensibles[788]. De hecho, cada vez es más frecuente que las empresas contraten a otras externas las cuales deben garantizar que el sistema utilizado para el almacenamiento de datos cumple con los preceptos de la LOPD. De esta forma, se evita que la empresa pueda tener algún tipo de responsabilidad por el tratamiento de esos datos, siendo, entonces, responsable la empresa contratada para este fin que pasa a ser la encargada del tratamiento[789].

---

[787] Art. 103 del RDLOPD: "*4. El período mínimo de conservación de los datos registrados será de dos años. 5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados. 6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias: a) Que el responsable del fichero o del tratamiento sea una persona física. b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales. La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad".*

[788] Vid., apartado 4.2.1 y 4.2.2 del presente Capítulo.

[789] SALOMON, D.: *Data privacy and security*, Springer, Nueva York, 2003, pp. 19 y ss.; DEL PESO NAVARRO, E. Y RAMOS GONZÁLEZ, M.A.: *Confidencialidad y seguridad en la información: la LORTAD y sus implicaciones socioeconómicas*, Díaz-Santos, Madrid, 1994, pp. 14 y ss.; DAVARA RODRÍGUEZ, M.A.: *Seguridad de los datos, nuevas tecnologías, sociedad y trabajo*, FUNDESCO, Madrid, 1991, pp. 38 y ss.; LUJAN ALCARAZ, J.: "Protección de datos de carácter personal y contrato de trabajo", *Revista Doctrinal Aranzadi Social,* núm. 7, 2003, pág.10.

Por esta razón se hace necesario identificar y conocer los distintos sujetos encargados de gestionar esas bases de datos; pues es obvio que en la gestión de los recursos humanos de la empresa intervienen otras personas distintas al empresario –asesores jurídicos, gestores, informáticos que crean y mantienen las bases de datos, etc.-, siendo éstos trabajadores los encargados de tratar los datos de acuerdo con lo previsto en la LOPD. Lógicamente, estos sujetos llegan a almacenar, también, datos de los trabajadores por lo que serán responsables igualmente si se produce en su actuación alguna vulneración de la normativa sobre protección de datos[790]. Este encargado de tratamiento también tiene que procurar proporcionar a los titulares de los datos las vías pertinentes para que puedan ejercer los derechos de acceso, rectificación, cancelación y oposición.

Como es sabido, esta responsabilidad del encargado del tratamiento se materializa en las obligaciones que contrae al firmar el contrato de hosting con el responsable del fichero, a través del cual se compromete a actuar diligentemente respecto a los datos que va a tratar conforme a un objetivo o finalidad concreto, incurriendo si no lo hiciera en las mismas responsabilidades que el responsable del fichero[791]. Si se dieran estas situaciones el empresario, que encarga la prestación de servicios, no es conocedor del tratamiento ilegítimo que se está haciendo de la información personal de los trabajadores, ya que no tiene el control de esas bases de datos por lo que parece evidente que la responsabilidad, en estos casos, la tengan estos sujetos externos a la empresa.

Ahora bien, acerca de la delegación de funciones que en un determinado momento el empresario realice con un trabajador de la empresa, relacionadas para el tratamiento y gestión del fichero de datos de carácter personal, habrá que delimitar si esa delegación es puntual o forma parte de la ejecución normal

[790] Art. 3.g) de la LOPD: *"Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".*

[791] Art. 12.4 de la LOPD: *"En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente".*

de tareas de ese trabajador. Si el empresario ordena al trabajador, en un momento concreto, el procesamiento de la información personal, cometido no acordado previamente entre sus funciones, la responsabilidad sobre posibles incumplimientos de la LOPD en el desarrollo del mandato la tendrá el propio empresario. Sin embargo, si estas actuaciones conforman la actividad diaria del trabajador, o ha sido contratado con esta finalidad, el empresario tendrá que dar instrucciones sobre el tratamiento de esos datos e incluso hacerle firmar una descripción de tareas y el compromiso de confidencialidad para efectuar esa prestación de servicios, incurriendo en la misma responsabilidad que un encargado del tratamiento. Esta delegación de funciones tendrá que quedar registrada en el documento de seguridad.

Lo mismo ocurre cuando esos datos de los trabajadores son cedidos a los distintos organismos encargados de validar el contrato de trabajo y otras de las muchas situaciones que tienen lugar en el desarrollo de la relación laboral, ya que estas entidades que reciben la información personal de los trabajadores, a veces especialmente sensibles, son ahora responsables de los ficheros que se crean al efecto. Pese a que la responsabilidad sobre esos datos cedidos pasa ahora a ser de otros sujetos –órganos administrativos, servicios de prevención, organizaciones sindicales etc.- no obstante, el empresario tendrá que realizar, en todo caso, esas transmisiones de datos a esas entidades cumpliendo los requisitos legales necesarios para que sean lícitas[792].

Obviamente tanto el responsable del fichero como el encargado del tratamiento, si no cumplen con las obligaciones citadas en los apartados anteriores – notificación del fichero ante el registro de la AEPD, observancia de los principios citados para el tratamiento de datos, implantación de medidas de seguridad etc.-, serán responsables de esos incumplimientos y de atender, a su vez, a la infracciones y sanciones reguladas en los arts. 42 y ss. de la LOPD[793].

[792] Vid. apartado 5 del presente Capítulo.
[793] Las infracciones que estipula la LOPD están catalogadas como leves, graves y muy graves a las cuales le corresponden sanciones que van de los 900 a los 600.000 euros según la calificación que tenga el incumplimiento de la normativa sobre protección de datos. No

4.3. Responsabilidad de los ficheros con datos especialmente protegidos de los trabajadores.

4.3.1. Responsabilidad de los ficheros con datos médicos de los trabajadores.

La cuestión de la responsabilidad adquiere tintes problemáticos en relación con los ficheros con datos médicos de los trabajadores debido a la variedad de sujetos implicados en su conocimiento –médicos, INSS, MCSS , empresario-, los cuales constituirán distintos ficheros con la información que están autorizados a recopilar; mayor o menor, más o menos sensible, según los casos .

Por ello, cuando el fichero soporte el almacenamiento de datos relativos a los resultados de estos exámenes médicos el responsable del fichero será el servicio de prevención pues, es quien decide sobre la finalidad, el contenido y uso que se le va a dar a los datos. Como es sabido, el empresario no está facultado para conocer ni registrar el contenido íntegro de estos reconocimientos médicos, indistintamente de que el servicio se cree dentro de su empresa[794] o contrate la prevención de los riesgos laborales con una empresa externa a la misma[795].

---

obstante, estas sanciones podrán graduarse atendiendo a los criterios del art. 45.4 de la LOPD.

[794] La doctrina científica ha establecido que los servicios de prevención propios o mancomunados no son entes independientes a la empresa, por lo que para articular mecanismos de protección de los datos será necesaria una delegación de funciones del responsable del fichero hacia una persona o personas integrante del servicio de prevención propio en: APARICIO SALOM, J.: *Estudio sobre la Ley Orgánica…*op. cit., pág. 33; ÁLVAREZ CIVANTOS, O.J.: Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*: (adaptación a la Ley 15/1999 de protección de datos de carácter personal y Reglamento de medidas de seguridad R.D. 994/1999),* Comares, 2001, pág. 169.

[795] Según la AEPD: *"En cuanto a la prestación de este tipo de servicios, en todo caso, y sin perjuicio de la categorización mercantil que merezca el contrato, debe señalarse que el mismo no encontrará amparo en lo establecido en el artículo 12 de la Ley Orgánica, toda vez que es preciso para que dicho precepto sea de aplicación que el tratante de los datos sea un mero encargado del tratamiento, que actúe en nombre y por cuenta del responsable, siendo así que el párrafo segundo del artículo 22.4 de la Ley 31/1995, al señalar que "El acceso a la información médica de carácter personal se limitará al personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador",* vid. Informe Jurídico 189/2008 de la AEPD, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes ._juridicos/conceptos/common/pdfs/2008-0189_Empresas-de-Prevenci-oo-n-de-Riesgos-

En cambio, si el fichero tan sólo incluye datos sobre las conclusiones de los reconocimientos médicos, la responsabilidad la tiene el empresario. Cosa distinta ocurre cuando el servicio de prevención está instalado en la propia empresa, ya que no es necesario crear otro fichero con estos datos relacionados con las conclusiones, puesto que el empresario ya lo ha establecido y se entiende que puede ser utilizado, también, por el personal del servicio de prevención de la propia empresa. Sin embargo, respecto a la vista de la habilitación legar para conocer y tratar los resultados de los reconocimientos médicos, este servicio de prevención propio sito en la empresa deberá contar con personal autorizado[796] para ello, es decir, personal sanitario[797], sin que puedan ser tratados por el empresario ni por otros trabajadores que no tengan esta catalogación

Por otra parte, cuando se registren datos relacionados con la incapacidad laboral de los trabajadores hay que atender a dos precisiones; en primer lugar, se creara un fichero en la empresa, el cual tendrá poco o ningún dato relacionado con la salud de los trabajadores, ya que el empresario sólo va a conocer la situación de baja laboral pero no el estado de salud ni las circunstancias médicas que rodean la ausencia temporal o permanente del trabajador en la empresa.

En segundo lugar, para la gestión de la incapacidad laboral, existe un fichero en el servicio médico que certifica la baja y otro en el INSS o en la correspondiente entidad colaboradora (MCSS. Estos sujetos son responsables del fichero de datos de salud de los trabajadores, con la peculiaridad de que, en el caso del INSS, se trata de una Administración Pública, por lo que el tratamiento datos por este organismo tiene algunas particularidades relacionadas con el cumplimiento de los principios de la LOPD en el tratamiento y cesión de datos[798].

Labora les-y-Mutuas-de-Accidente-son-responsables-del-tratamiento.pdf [Consulta 20/06/2015].

[796] Vid., art. 22.4 de la LPRL.

[797] PEDROSA ALQUEZAR, S.: "Confidencialidad y protección de datos en la vigilancia de la salud de los trabajadores: bases para una prevención de calidad" *Revista CEF, Estudios Financieros y de Seguridad Social*, núm. 21, 2004,pp. 27-29.

[798] Vid, apartado 5.1.2 del presente Capítulo.

En otro orden y relacionado con la responsabilidad de los ficheros de datos relacionados con el genoma humano y con aquellos derivados de la realización de test de alcoholemia o drogas será, también, el personal sanitario encargado de realizarlo, sin que el empresario pueda tener acceso a los resultados de esas pruebas médicas. Debido al carácter reservado de estos datos y a las consecuencias para el trabajador que puede conllevar su conocimiento por parte del empresario, tienen que ser únicamente tratadas por el personal sanitario encargadas de efectuar estos tests, aunque si el trabajador consiente expresamente su tratamiento por parte del empresario, éste si estaría habilitado para crear una base de datos con esa información, siempre que el empresario le advierta con que finalidad y sentido quiere hacer uso de esa información acerca de su estado de salud.

Los responsables de los ficheros de datos están obligados a guardar la debida confidencialidad[799] sobre todas las informaciones contenidas en sus bases de datos. Pero, cuando los datos son relativos a los resultados de los exámenes médicos, están obligados a la observancia del secreto profesional sobre esos datos además los profesionales sanitarios, encargados del fichero con esa información, También, la LPRL[800] establece la obligación de confidencialidad respecto de aquellos datos manejados por las personas encargadas del servicio de prevención de la empresa, los cuales sólo deben ser conocidos por los trabajadores que intervienen en las prácticas de esas pruebas y los documentalistas que los incorporan al soporte papel o informático, pero no por aquellas personas ayudantes de esos profesionales. No sólo se establece este deber de sigilo para los resultados de los reconocimientos médicos, sino también para todas aquellas informaciones que

[799] Art. 10 de la LOPD: *"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".*

[800] Art. 22.2 de la LPRL: "*Las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo respetando siempre el derecho a la intimidad y a la dignidad de la persona del trabajador y la confidencialidad de toda la información relacionada con su estado de salud".*

el trabajador haya podido confiar al médico o a aquellas personas involucradas en las tareas preventivas[801].

El incumplimiento de las obligaciones de los responsables, respecto a la preservación de los datos médicos de los trabajadores, puede generar responsabilidades civiles en cuanto a la indemnización por daños[802] que se pueda establecer por la vulneración del derecho a la protección de datos de cualquier ciudadano, en este caso del trabajador. Por su parte, la responsabilidad administrativa en el ámbito preventivo, y respecto al archivo de los datos de salud de los trabajadores, viene establecida en el del RD 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el orden social[803] considerando, en su art. 12.4, una infracción grave el hecho de no registrar y archivar los datos obtenidos en los reconocimientos médicos.

También se puede incurrir en otra infracción administrativa, calificada como muy grave, si el responsable no cumple con el debido sigilo profesional en el tratamiento de datos relativos a la salud de los trabajadores[804]. Por otra parte, conviene no olvidar que estas infracciones también tienen presencia y sanción en la LOPD[805], por lo que un mismo hecho cometido por un mismo sujeto da lugar a dos infracciones reguladas en dos normas distintas

[801] RODRÍGUEZ ESCANCIANO, S. Y FERNÁNDEZ DOMÍNGUEZ, J.J.: Utilización y control de datos laborales…,op.cit., pp. 195-201; SAN MARTÍN MAZZUCCONI, C.: "La vigilancia del estado de salud de los trabajadores: voluntariedad y periodicidad…", op. cit., pp. 181-202; SÁNCHEZ CARAZO, C .: La intimidad y el secreto médico, Díaz de Santos, 2000, pp. 196-204; BLASCO PELLICER, A.: "El deber empresarial de vigilancia de la salud y el derecho a la intimidad del trabajador" en VV.AA.: *Trabajo y Libertades Públicas*, Madrid, La Ley-Actualidad, 1999, pp. 274-275; SÁNCHEZ TORRES, E.: "El derecho a la intimidad del trabajador en la Ley de Prevención de Riesgos Laborales" *Revista Relaciones Laborales*, núm. 2, 1997, pág.459.

[802] Art. 19 de la LOPD: *"1.Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados. 2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria".*

[803] BOE núm. 189 de 8 de agosto de 2000.

[804] Art. 13.5 del TRLISOS: *"Incumplir el deber de confidencialidad en el uso de los datos relativos a la vigilancia de la salud de los trabajadores, en los términos previstos en el apartado 4 del artículo 22 de la Ley de Prevención de Riesgos Laborales".*

[805] Art. 44.4 b) de la LOPD: "*Tratar o ceder los datos de carácter personal a los que se refieren los apartados 2, 3 y 5 del artículo 7 de esta Ley salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del artículo 7".*

resolviendo, en este caso, el órgano al que se le haya presentado la denuncia o aquél que primero haya averiguado, a través de sus mecanismos de inspección, la posible infracción[806].

A la hora de imputar la responsabilidad sobre la inobservancia de los principios tasados en la LOPD –calidad, información y consentimiento- en el registro de la información médica, habrá que distinguir si ésta pertenece al empresario[807] –conclusiones- o si por el contrario es la empresa externa encargada de la PRL –resultados-. Si como consecuencia de la falta de registro de datos se pudiera acarrear un riesgo grave para la integridad física o la salud de los trabajadores el servicio de prevención, contratado por la empresa y habilitado para el tratamiento de esta información, puede en una infracción grave tipificada en el art. 12.16. i) del TRLISOS[808], si como consecuencia de la falta del registro de datos se pudiera acarrear un riesgo grave para la integridad física o la salud de los trabajadores, siendo la sanción pertinente para este tipo de ilícitos la prevista en el art. 40.2 b) del TRLISOS[809]

4.3.2. Responsabilidad de los ficheros con datos acerca de la afiliación sindical de los trabajadores.

Al margen de la responsabilidad de los ficheros con datos de afiliación sindical de los trabajadores que tienen las organizaciones sindicales que son aquellas que se encargan de realizar la administración de los afiliados[810] y, por

[806] SIERRA HERNÁIZ, E.: "Los sujetos responsables en el marco de las infracciones administrativas en materia de prevención de riesgos laborales" *Tribuna Social: Revista de Seguridad Social y laboral*, núm. 239, 2010.pp. 28-38; FERNÁNDEZ MÁRQUEZ, O. Y GARCÍA MURCIA J.: "Infracciones extra sistemáticas del empresario en materia social" *Revista del Ministerio de Trabajo e Inmigración,* núm. 78, 2008, pp. 75-77; CAMAS RODA, F.: "Las infracciones y sanciones administrativas del empresario en el orden social", Estudios financieros. Revista de Trabajo y Seguridad Social, núm. 254, 2004, pp. 36-41.

[807] Se establecen las mismas infracciones y sanciones que para el tratamiento ilícito del cualquier dato de carácter personal (Vid., art. 42 y ss de la LOPD).

[808] Art.12.16. i) del TRLISOS: "*Las que supongan incumplimiento de la normativa de prevención de riesgos laborales, siempre que dicho incumplimiento cree un riesgo grave para la integridad física o la salud de los trabajadores afectados y especialmente en materia de: Registro de los niveles de exposición a agentes físicos, químicos y biológicos, listas de trabajadores expuestos y expedientes médicos".*

[809] Art. 40.2 b): *"Las graves con multa, en su grado mínimo, de 2.046 a 8.195 euros; en su grado medio, de 8.196 a 20.490 euros; y en su grado máximo, de 20.491 a 40.985 euros".*

[810] En el caso de la organizaciones sindicales la configuración de estos ficheros podría justificarse en la necesidad de registrar esos datos no con la única finalidad de almacenarlos, sino para velar por los intereses de esos trabajadores afiliados y llevar un control, también, de las empresas en las que están trabajando para poder constatar que se respetan sus derechos

tanto, de generar una base de datos con esta información. Existen supuestos, que se desarrollan dentro del ámbito organizativo empresarial[811], en los que se pueden crear ficheros con información acerca de la pertenencia del trabajador a un sindicato, y es aquí donde el empresario tiene la responsabilidad de velar por el tratamiento adecuado de esos datos.

El archivo de estos datos por el empresario, lo que lo convierte en responsable de los mismos , ha de hacerse, como se ha indicado ya, solicitando la previa conformidad del propio trabajador, el cual no está obligado a darla como así se establece en el art. 16 CE[812], sin que su negativa u ocultación pueda suponer un perjuicio para él. Si los datos los solicita el empresario a los propios sindicatos, se estaría produciendo una cesión de datos de los trabajadores, que tendría que estar rodeada de las garantías previstas en la normativa sobre protección de datos de carácter personal[813].

Cualquier registro de la información sindical de los trabajadores que el empresario realice sin cumplir las exigencias de la LOPD y sin que mediara el consentimiento expreso y por escrito del trabajador para ello, estaría vulnerando el derecho a la protección de datos del trabajador realizando un tratamiento no permitido de los datos relacionados con su afiliación sindical. En este caso, este empresario sería responsable del tratamiento ilícito de estos datos incurriendo en una infracción grave del art. 44.3 b) de la LOPD[814], pudiendo ser sancionado con una multa de entre 40.001 a 300.000 euros[815].

---

laborales. Obviamente, sin estas bases de datos sería muy complicado que los sindicatos pudieran ejercer sus funciones, como consecuencia de la gran cantidad de afiliados que pueden tener y las pocas posibilidades de supervisar sus inquietudes si no cuentan con un fichero con esa información.

811 Estos casos están descritos en el apartado 2.2 del presente Capítulo.

812 Art.16 de la CE: "Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias."

813 En este sentido; RODRÍGUEZ ESCANCIANO, S.: "El derecho a la protección de datos personales…, op. cit., pp. 67-70; TRONCOSO REIGADO, A.: *La protección de datos…,*op. cit., pp.1570-1572; THIBAULT ARANDA, J.: "La intimidad informática del trabajador. Novedades de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal" en DAVARA RODRÍGUEZ, M.: *Jornadas sobre Informática y Sociedad,* Comillas, Madrid, 2001, pp. 224-225.

814 Art. 44.3 b): "*Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo".*

815 Vid. art. 45.2 de la LOPD.

5. LAS CESIONES DE DATOS DE TRABAJADORES EN EL MARCO DE LA RELACIÓN LABORAL.

Basta una mera aproximación al análisis de las situaciones que se dan en las relaciones de trabajo para comprobar la necesidad que existe de realizar transmisiones de datos de los trabajadores de forma casi constante. La inmensa mayoría de esas comunicaciones de información las realiza el empresario, ya que es el que tiene en su poder esa información que ha obtenido legalmente y que le ha facilitado (debiendo mediar o no consentimiento para ello) previamente el trabajador.

Una de las vías de transmisión es la que conecta a la empresa con las Administraciones Públicas. La posibilidad de hacer trámites a través de la Administración Electrónica se ha convertido en un mecanismo imprescindible para realizar las numerosas gestiones administrativas relacionadas con los trabajadores de una forma mucho más ágil y eficaz[816]. Es en la propia normativa que regula la Administración Electrónica[817] donde se hace alusión a la utilización de las TICs como medio de transmisión de datos a la Administración y al respeto a las exigencias establecidas en la LOPD y en el RDLOPD[818].

---

816 Art. 1 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (BOE núm. 150 de 23 de junio de 2007): *"La presente Ley reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica".*

817 Sobre la Administración Electrónica vid., BARNÉS VÁZQUEZ, J.: *Innovación y reforma en el Derecho Administrativo,* Ed. Derecho Global, 2006, pág. 131 y ss.; HERNÁNDEZ CORCHETE, J.A.*: "El derecho de los ciudadanos a relacionarse con las administraciones públicas utilizando los medios electrónicos y los derechos complementarios que delimitan su alcance" en* PIÑAR MAÑAS, J.L. (coord.): *Transparencia, acceso a la información y protección de datos,* Reus, 2014, pp. 98-100. INAP: *Libro Blanco sobre la administración electrónica y la protección de datos, Ministerio de Administraciones Públicas,* 2001, pp.37-43; GUTIÉRREZ MARTÍNEZ, R.: *La Administración Pública electrónica*, Civitas, 2009, pp. 52-55, 65-67*;* DEL CASTILLO VÁZQUEZ, I.C.: *"Transparencia, acceso a la documentación administrativa y protección de datos de carácter personal", Foro Nueva Época,* núm. 6, 2007, pp. 249-250*.*

818 Art. 4.1 a) de la LAECSP: *"El respeto al derecho a la protección de datos de carácter personal en los términos establecidos por la Ley Orgánica 15/1999, de Protección de los Datos de Carácter Personal, en las demás leyes específicas que regulan el tratamiento de la información y en sus normas de desarrollo, así como a los derechos al honor y a la intimidad personal y familiar".*

Otra vía de comunicación de datos es la que conecta la empresa con los representantes de los trabajadores (unitarios o sindicales), transmitiéndoles informaciones, que pueden alcanzar el rango de datos personales, con la finalidad de favorecer el ejercicio de dicha representación así como las funciones vinculadas a la defensa de los intereses de los propios trabajadores.[819]. Por lo que es imprescindible examinar también en qué circunstancias estas comunicaciones se realizan siguiendo lo establecido en la normativa sobre protección de datos acerca de las cesiones de información.

5.1. Mecanismos de transmisión de datos personales de los trabajadores desde la empresa a la Administración Pública.

Una de las primeras gestiones que tiene que realizar el empresario con los datos facilitados por el trabajador es la configuración de su contrato de trabajo, para acto seguido comunicar esos contratos de trabajo, a los organismos encargados de realizar su registro. Aunque, de forma preliminar, hay que fijar qué datos son los previstos para la cesión a los distintos organismos - Seguridad Social, Administración Tributaria y SEPE- para poder acreditar que se trata efectivamente de informaciones que revisten el carácter de personales.

Cuando el empresario quiere dar de alta al trabajador en el Régimen General de la Seguridad Social tiene que trasladar a la TGSS la siguiente información[820]: nombre o razón social del empresario que promueve el alta; Código de Cuenta de Cotización del empresario; régimen de Seguridad Social;

[819] Art. 64.1 del ET: *"El comité de empresa tendrá derecho a ser informado y consultado por el empresario sobre aquellas cuestiones que puedan afectar a los trabajadores, así como sobre la situación de la empresa y la evolución del empleo en la misma, en los términos previstos en este artículo. Se entiende por información la transmisión de datos por el empresario al comité de empresa, a fin de que este tenga conocimiento de una cuestión determinada y pueda proceder a su examen. Por consulta se entiende el intercambio de opiniones y la apertura de un diálogo entre el empresario y el comité de empresa sobre una cuestión determinada, incluyendo, en su caso, la emisión de informe previo por parte del mismo. En la definición o aplicación de los procedimientos de información y consulta, el empresario y el comité de empresa actuarán con espíritu de cooperación, en cumplimiento de sus derechos y obligaciones recíprocas, teniendo en cuenta tanto los intereses de la empresa como los de los trabajadores*".

[820] Vid., art. 30.2 del Real Decreto 84/1996, de 26 de enero, por el que se aprueba el Reglamento general sobre inscripción de empresas y afiliación, altas, bajas y variaciones de datos de trabajadores en la Seguridad Social (BOE núm. 50 de 27 de febrero de 1996).

apellidos y nombre del trabajador; número de Seguridad Social del trabajador; DNI; domicilio del trabajador; fecha de inicio de la actividad; grupo de cotización; epígrafe de accidente de trabajo y enfermedad profesional; tipo de contrato y coeficiente de jornada en su caso; y ocupación, tan sólo en los supuestos indicados en la Disposición adicional cuarta de la Ley 42/2006 de 28 de diciembre de 2006, de Presupuestos Generales del Estado para el año 2007[821]. Lógicamente, este trabajador tendrá que tener el número de afiliación a la Seguridad Social para poder ser dado de alta ya que, si no lo tuviera, tiene que solicitarlo a la Tesorería General de la Seguridad Social, que lo incluirá en el Sistema de Seguridad Social[822].

Las transmisiones de datos para hacer efectiva el alta del trabajador se pueden hacer a través de medios electrónicos, siendo el sistema RED (remisión electrónica de documentos) el utilizado en el ámbito de la Administración de la Seguridad Social[823]. Este sistema está habilitado para realizar distintas comunicaciones de datos de forma electrónica[824] y, para su realización, es necesario que el empresario, en este caso, esté en disposición de alguno de los mecanismos de autenticación establecido en la Ley 11/2007[825], siendo el necesario para hacer gestiones a través del sistema RED

[821] BOE núm. 311 de 29 de diciembre de 2006.
[822] PLANAS GÓMEZ, M.: *Gestión Práctica de la Seguridad Social*, CISS, 2007, pp.127-128; MARTÍNEZ LUCAS, J.A.: "El alta de los trabajadores en la Seguridad Social", Revista General de Derecho, núm.625-626, 1996, pp. 11.285-11.322; CAMPELO LÓPEZ, O.: "Los actos de encuadramiento en el sistema de la Seguridad Social: inscripción de empresas y afiliación, altas y bajas de los trabajadores" en MELLA MÉNDEZ, L. Y GARCÍA ROJO, A. (coord.): *Prácticas de la Seguridad Social,* La Ley, 2011, pp. 49-58.
[823] Orden ESS/484/2013, de 26 de marzo, por la que se regula el Sistema de remisión electrónica de datos en el ámbito de la Seguridad Social (BOE núm. 75 del 28 de marzo de 2013).
[824] Véase art. 1.1 de la Orden ESS/484/2013.
[825] Art. 13 de la LAECSP: "1*. Las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y resulten adecuados para garantizar la identificación de los participantes y, en su caso, la autenticidad e integridad de los documentos electrónicos. 2. Los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las Administraciones Públicas, de acuerdo con lo que cada Administración determine: a) En todo caso, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas. b) Sistemas de firma electrónica avanzada basados en certificados electrónicos reconocidos. Las Administraciones Públicas deberán admitir todos los certificados reconocidos incluidos en la "Lista de confianza de prestadores de servicios de certificación" (TSL) establecidos en España, publicada en la sede electrónica del Ministerio de Industria, Energía y Turismo. c) Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de*

el certificado SILCON[826]. Además de este certificado, para operar en la plataforma RED, se hace preciso contar con la autorización de la TGSS[827], la cual debe concederse para actuar en nombre propio o en nombre de un tercero, dependiendo de las funciones que vaya a efectuar por medio de este mecanismo[828].

Por otra parte, el trabajador, una vez contratado, debe cumplimentar el modelo 145 de retenciones por rendimientos del trabajo las cuales le va a practicar el empresario cuando proceda al pago mensual de su nómina. Este formulario debe contener información, además de los datos identificativos del trabajador, acerca de su situación familiar; discapacidad; movilidad geográfica; los hijos menores de 25 años que convivan con él; los ascendientes mayores de 65 años que vivan en su domicilio; y el pago de alguna pensión compensatoria en caso de separación o divorcio. En este caso, es el trabajador

---

información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen".

826 El certificado SILCON sirve para la actualización y consulta de datos por parte de representantes de empresas y expresamente para el Sistema RED. Para obtener este certificado proporcionado por la Seguridad Social siga el siguiente procedimiento: El usuario deberá personarse en una Oficina de certificados digitales, identificándose con su DNI, pasaporte o con el NIE en caso de ser extranjero. El registrador recogerá los datos necesarios para realizar el registro: nombre y apellidos; NIF; domicilio; teléfono, fax, o correo electrónico. Una vez comprobados que los datos son correctos, se entregará al interesado dos copias del contrato, que deberá firmar tras comprobar que están debidamente cumplimentadas con sus datos personales, conservando una el usuario y archivándose la otra en la oficina de registro. Junto con la copia del contrato, el usuario recibirá un disquete que contiene el certificado y un sobre con una hoja impresa con los ocho caracteres de la contraseña del certificado. Cada vez que un usuario acceda a los servicios del RED, Mutuas Colaboradoras con la Seguridad Social, Centros Públicos de Salud o Instituto Cervantes, se les mostrará una pantalla en la que se solicitará el archivo .epf, que se encuentra en el disquete que se les entregó y la contraseña asociada al certificado. Fuente: http://www.seg-social.es/Internet_1/Sede/Certificadosdigital47735/Certificadosparalos51671/index.htm [Consulta 2/07/2015].

827 Art. 5.1. de la Orden ESS/484/2013: *"1. Para operar en el ámbito de actuación definido en el artículo 1, será necesario contar con autorización otorgada por la Tesorería General de la Seguridad Social. Dicha autorización podrá ser de dos tipos: a) Autorización para actuar en nombre propio. b) Autorización para actuar en nombre de otros. La Tesorería General de la Seguridad Social determinará mediante resolución del Director General los requisitos que se han de cumplir para la obtención de cada tipo de autorización".*

828 Acerca del sistema RED, vid., HIERRO HIERRO, F.J.: "Una aproximación al sistema de red de la Tesorería General de la Seguridad Social", *Revista Aranzadi Social*, núm. 2, 2003, pp. 1-2; QUINTERO LIMA, M.G.: "El uso de medios electrónicos, informáticos y telemáticos en relación con los actos de gestión de seguridad social: el sistema de remisión electrónica de datos (sistema red)" *Revista de la contratación electrónica*, núm. 61, 2005, pp. 69-94; VALVERDE ASENCIO, A. J.: RL. "Algunas cuestiones sobre el marco normativo del Sistema de Remisión Electrónica de Documentos a la Tesorería General de la Seguridad Social" *Revista Relaciones Laborales*, núm. 1, 2002, pp. 1497 y ss.; MAGALLÓN ORTÍN, M.: "Intercambio electrónico de dato en materia de afiliación y recaudación de Seguridad Social (Proyecto RED)", *Revista de Trabajo y Seguridad Social*, núm. 18, 1995, pág. 150.

el que comunica esa información[829] al empresario para que éste lo notifique a la Agencia Estatal de Administración Tributaria[830]. La forma de transmitir esta información también puede realizarse de forma telemática[831] a través de la sede electrónica de la AEAT[832]. Al igual que ocurre con el sistema RED, para hacer gestiones por medio de los servicios telemáticos de la AEAT, concretamente para comunicar el modelo 145, el empresario tendrá que estar en posesión de alguno de los mecanismos de autenticación permitidos en la sede electrónica de la AEAT como: un certificado digital expedido por la FNMT[833]; el número de referencia y/o casilla; la clave pin 24 horas; u otros sistemas de identificación[834].

Otra de las gestiones que tendrá que realizar el empresario cuando procede a la contratación del trabajador es la comunicación de la copia básica del contrato al SEPE[835]. A través del servicio Contrat@, inserto en la sede

[829] Los datos que tiene que cumplimentar el trabajador en el citado modelo 145 son; datos identificativos; información sobre su situación familiar relacionada con la posibilidad de tener descendientes o ascendientes a su cargo; información sobre los pagos que realiza (pensiones a favor de cónyuge o hijos y préstamos destinados a pagar su vivienda habitual).

[830] Art. 88 del Real Decreto 439/2007: "*Los contribuyentes deberán comunicar al pagador la situación personal y familiar que influye en el importe excepcionado de retener, en la determinación del tipo de retención o en las regularizaciones de éste, quedando obligado asimismo el pagador a conservar la comunicación debidamente firmada".*

[831] Art. 88.1 del RD 439/2007: *"La comunicación a que se refiere el párrafo anterior también podrá efectuarse por medios telemáticos o electrónicos siempre que se garanticen la autenticidad del origen, la integridad del contenido, la conservación de la comunicación y la accesibilidad por parte de la Administración tributaria a la misma".*

[832] https://www.agenciatributaria.gob.es/AEAT.sede/tramitacion/G603.shtml.

[833] Vid., nota a pie 70, en dónde se establece la forma de expedición de estos certificados.

[834] OLIVER CUELLO, R.: "La sede electrónica de la Agencia Estatal de Administración Tributaria" *IDP: Revista de Internet, Derecho y Política,* núm. 12, 2011, pp. 46-48.

[835] En el art, 8.4 del ET se contemplan las cesiones de la copia básica del contrato de trabajo, haciendo referencia a los datos que deben estar insertos en la misma y al cumplimiento de lo establecido en la normativa sobre protección de datos: *"El empresario entregará a la representación legal de los trabajadores una copia básica de todos los contratos que deban celebrarse por escrito, a excepción de los contratos de relación laboral especial de alta dirección sobre los que se establece el deber de notificación a la representación legal de los trabajadores. Con el fin de comprobar la adecuación del contenido del contrato a la legalidad vigente, esta copia básica contendrá todos los datos del contrato a excepción del número del documento nacional de identidad o del número de identidad de extranjero, el domicilio, el estado civil, y cualquier otro que, de acuerdo con la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, pudiera afectar a la intimidad personal. El tratamiento de la información facilitada estará sometido a los principios y garantías previstos en la normativa aplicable en materia de protección de datos. La copia básica se entregará por el empresario, en plazo no superior a diez días desde la formalización del contrato, a los representantes legales de los trabajadores, quienes la firmarán a efectos de acreditar que se ha producido la entrega. Posteriormente, dicha copia básica se enviará a la oficina de empleo. Cuando no exista representación legal de*

electrónica del SEPE[836], se permite a los empresarios comunicar el contenido de los contratos de trabajo a los SEPE[837] desde su propio despacho o sede profesional. La utilización de este servicio requiere disponer de permiso de los SEPE y, para ello, se deberá cumplimentar la solicitud de autorización y presentarla con la documentación precisa en dichas entidades o disponer de un certificado digital expedido por la FNMT.

5.1.1. Requisitos necesarios para la cesión de datos a las Administraciones Públicas.

Todas las comunicaciones de datos de trabajadores a los organismos administrativos citados[838] se pueden analizar desde dos puntos de vista: por un lado, las que realiza el empresario al órgano administrativo que corresponda; y por otro, las que pueden realizar las propias Administraciones Públicas a otros organismos sobre la información de los trabajadores almacenada en sus propios ficheros[839].

Teniendo en cuenta, en primer lugar, las cesiones que efectúa el empresario a la Administración Pública hay que afirmar , como criterio general, que todas estas cesiones tienen que cumplir con el principio de calidad de los datos y, por tanto, deben efectuarse con la intención exclusiva y la funcionalidad relevante de practicar hacer las gestiones administrativas vinculadas al contrato de trabajo. En consecuencia, el empresario no podrá

---

los trabajadores también deberá formalizarse copia básica y remitirse a la oficina de empleo. Los representantes de la Administración, así como los de las organizaciones sindicales y de las asociaciones empresariales, que tengan acceso a la copia básica de los contratos en virtud de su pertenencia a los órganos de participación institucional que reglamentariamente tengan tales facultades, observarán sigilo profesional, no pudiendo utilizar dicha documentación para fines distintos de los que motivaron su conocimiento".

[836] https://www.sepe.es/contenidos/OficinaVirtual/info_contrata.html [Consulta 01/07/2015].

[837] La informatización de los SEPE vino de la mano de la Orden TAS/503/2007, de 28 febrero, por la que se creó un registro telemático en el SEPE para la presentación de escritos, solicitudes y comunicaciones, a la vez que se establecían los criterios generales para la tramitación telemática de determinados procedimientos. Esta norma habilitó por primera vez al SEPE la utilización de las TICS en la presentación de escritos y tramitación de procedimientos, con el objetivo de crear un sistema que facilitara la comunicación del citado servicio con otras administraciones y, fundamentalmente, con los ciudadanos.

[838] Vid., apartado 2.1 del presente capítulo.

[839] Obviamente el contenido de estos ficheros es una consecuencia directa de las comunicaciones efectuadas por el empresario y por este motivo, se va a analizar la gestión de estos ficheros y las exigencias que le impone la LOPD en el apartado 2.1.2. del presente capítulo.

comunicar a la Administración Pública los datos personales, contenidos en el contrato de trabajo y pertinentemente fichados, con una finalidad diferente, como tampoco los que no le sean requeridos por la propia AP destinataria de la cesión y que no estén funcionalizados, según los casos, a comunicar la situación de alta del trabajador en la empresa, las retenciones por rendimiento de trabajo, o registrar el contrato en el SEPE. La acción empresarial de revelar la información personal del trabajador arriba reseñada debe ir acompañada de la advertencia al titular del dato sobre la realización de estas cesiones, para que esté informado de la creación de un nuevo fichero de datos, ahora en el marco de la Administración Pública[840].

En principio, para notificar datos a terceros, el cedente (el empresario) debe requerir el consentimiento al interesado o titular del dato (el trabajador). Pudiendo deducirse del principio de información que el empresario, entre todas las advertencias que le debe dar al trabajador acerca del tratamiento de sus datos de carácter personal, debe informarle también sobre las posibles cesiones de datos que se van a realizar, anunciando las que tiene que realizar el empresario a la Administración Pública, por lo que podría sobreentenderse que se ha prestado el consentimiento también para esa comunicación[841].

Aun así, se puede dar algún supuesto en el que se puedan comunicar los datos de los trabajadores a los órganos administrativos sin necesidad de requerir su consentimiento. Esto se produce como consecuencia de lo establecido en el art. 11.2 a) de la LOPD, en el que se permite la comunicación de datos sin la conformidad del interesado cuando ésta se encuentre autorizada por una Ley. Por tanto, se podrán realizar estas transmisiones de datos a la Administración de la Seguridad Social[842] y a la AEAT[843] pues,

[840] Vid., apartado 5.1.2. del presente Capítulo.
[841] TRONCOSO REIGADA, A.: "La Comunicación de datos personales" en VV.AA.: *Comentario a la Ley Orgánica de Protección de datos,* Thomson-Reuters, 2010, pp. 959-960.
[842] Art. 29.1.1º del RD 84/1996: *"1. Con independencia de la obligación de solicitar la afiliación al Sistema de la Seguridad Social de los trabajadores no afiliados al mismo que hayan de ingresar o ingresen a su servicio, los empresarios estarán obligados a comunicar la iniciación o, en su caso, el cese de la prestación de servicios de los trabajadores en su empresa para que sean dados, respectivamente, de alta o de baja en el Régimen en que figuran incluidos en función de la actividad de aquélla, en los términos y condiciones establecidos en este Reglamento".*

además de ser autorizadas por una norma, se trata de obligaciones que tiene que cumplir el responsable del fichero en este caso, el empresario[844]. Lo mismo ocurre con la cesión de datos relativos a la copia básica del contrato de trabajo a los SEPE, ya que está es una obligación empresarial contenida en el art. 8 del ET.

En otro orden de cosas, y una vez que los datos están en poder de la correspondiente Administración Pública, la LOPD[845] establece que para realizar comunicaciones entre estas entidades públicas no será preciso el consentimiento del titular del dato, siempre que éstas tengan como objetivo ceder datos a otras Administraciones Públicas y no a órganos dependientes de

---

[843] Art. 99.2 de la Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas y de modificación parcial de las leyes de los Impuestos sobre Sociedades, sobre la Renta de no Residentes y sobre el Patrimonio (BOE núm. 285 de 29 de noviembre de 2006) : *"2. Las entidades y las personas jurídicas, incluidas las entidades en atribución de rentas, que satisfagan o abonen rentas sujetas a este impuesto, estarán obligadas a practicar retención e ingreso a cuenta, en concepto de pago a cuenta del Impuesto sobre la Renta de las Personas Físicas correspondiente al perceptor, en la cantidad que se determine reglamentariamente y a ingresar su importe en el Tesoro en los casos y en la forma que se establezcan. Estarán sujetos a las mismas obligaciones los contribuyentes por este impuesto que ejerzan actividades económicas respecto a las rentas que satisfagan o abonen en el ejercicio de dichas actividades, así como las personas físicas, jurídicas y demás entidades no residentes en territorio español, que operen en él mediante establecimiento permanente, o sin establecimiento permanente respecto a los rendimientos del trabajo que satisfagan, así como respecto de otros rendimientos sometidos a retención o ingreso a cuenta que constituyan gasto deducible para la obtención de las rentas a que se refiere el apartado 2 del artículo 24 del texto refundido de la Ley del Impuesto sobre la Renta de no Residentes".*

[844] Art. 10.2 a) del RD 1720/2007: *"2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando: a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes: El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre".*

[845] Art. 21 de la LOPD: "*1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. 2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra. 3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa. 4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley*".

esa misma administración[846]. Aunque sobre este aspecto quizás se pueda realizar alguna matización en torno al cumplimiento del principio de calidad, ya que si se traslada la información de los trabajadores a otras Administraciones Públicas es posible que se utilicen para otras finalidades que puedan ser incompatibles con el objetivo inicial que propició la recogida del dato. En estos casos, la doctrina ha estimado la valoración en sentido amplio del principio de calidad, es decir, la permisibilidad en lo relativo al tratamiento del dato para otros fines distintos de los iniciales pero siempre que guarden relación con la administración de personal[847].

Siguiendo este planteamiento, y en lo que a la contratación de trabajadores se refiere, obviamente, se producen comunicaciones de datos dentro de los organismos citados a otras entidades administrativas– Administración de la Seguridad Social[848], AEAT y SEPE- para poder llevar a cabo, no sólo el registro del contrato de trabajo, sino todas aquellas actuaciones que se deriven de la prestación de la relación laboral iniciada[849].

---

[846] En este sentido; TRONCOSO REIGADA, A.: "La administración electrónica y la protección de datos" *Revista Jurídica de Castilla y León, 2008*, pp. 71 y 91; GUICHOT REINA, E.: *Datos personales y Administración Pública*, Thomson-Civitas, 2005, pág. 247; SOUVIRÓN MORENILLA, J.M.: "En torno a la juridificación del poder informativo del Estado y el control de datos por la Administración", *Revista Vasca de Administración Pública*, núm. 40, 1994, pág.168. En contra de este planteamiento vid., GAY FUENTES, C.: *Intimidad y tratamiento de datos en las Administraciones Públicas,* Universidad Complutense, Madrid, 1995, pp. 97-99.

[847] FERNÁNDEZ SALMERÓN, M.: *La protección de datos en la Administración Pública*, Civitas, 2003, pág. 232. GONZÁLEZ NAVARRO, F.: "La relación jurídica de disposición de datos de carácter personal" en VV.AA.: *El derecho a la intimidad y a la privacidad y las administraciones públicas*, Escola Galega de Administración Pública, 1999, pp. 66-67.

[848] Art. 53 del RD 84/1996: *"Los datos obrantes en los registros y sistemas de documentación a que se refiere el artículo anterior serán utilizados por las entidades gestoras y servicios comunes de la Seguridad Social para los fines de los mismos, sin perjuicio de que deban facilitarse a otras Administraciones públicas en los términos previstos en el artículo 4 de la Ley 30/1992, de 26 de noviembre, y, en especial, a las Administraciones tributarias conforme a lo previsto en el artículo 36.6 del texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto legislativo 1/1994, de 20 de junio, así como a las comisiones parlamentarias de investigación de acuerdo con lo dispuesto en el Real Decreto legislativo 5/1994, de 29 de abril, y a los sindicatos con capacidad de promoción de elecciones en los términos establecidos en el artículo 67 del texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto legislativo 1/1995, de 24 de marzo, y en los demás casos en que así se establezca por Ley o en ejecución de ella".*

[849] En este sentido véase lo establecido en el art. 8.2 de la Recomendación CM/Rec del Comité de Ministros de la UE sobre el tratamiento de datos personales en el contexto del empleo de 1 de abril de 2015, en el que se admite la cesión de datos a organismos públicos cuando ésta tenga como finalidad otros aspectos no relacionados con sus funciones oficiales deberá cumplir una serie de requisitos: a) que sea necesaria para fines de empleo, los efectos no son incompatibles con los fines para los que los datos fueron recogidos inicialmente y si el empleado en cuestión o sus representantes, según el caso, haya sido informado de esto por

Por este motivo, estas comunicaciones, de datos de trabajadores se realizan sin necesidad de consentimiento pero siempre deben hacerse a Administraciones Públicas que traten materias afines o idénticas al órgano administrativo cedente[850]. De hecho, se puede admitir la cesión sin consentimiento si, por ejemplo, lo que pretende la administración receptora es tratar esa información con fines estadísticos, históricos o científicos; o se constituya como organismo que recaba datos y los transmite a otra, estando esta información disponible para el titular del dato[851]; o cuando la comunicación de datos tiene como destino la Administración de justicia o el Defensor del pueblo para solucionar algún conflicto que sólo estos organismos puedan resolver[852].

Las consecuencias jurídicas derivadas de la falta de cumplimiento de lo previsto en la LOPD por parte de la Administración son la imposición de la correspondiente sanción[853] como consecuencia de la realización de una

---

adelantado; b) con el consentimiento expreso, libre e informado del trabajador de que se trate; c) si se está prevista la comunicación en la legislación interna y, en particular, cuando sea necesario a los efectos de la ejecución de obligaciones legales o de acuerdo con los convenios colectivos.

[850] Análogamente la AEPD ha establecido que: "*En conclusión, la cesiones previstas entre ambos organismos se encuentran amparadas en el artículo 21.1 de la Ley Orgánica 15/1999 en caso de que la los datos se utilicen única y exclusivamente para las finalidades vinculadas con el ejercicio de potestades de derecho público y se incorporen a los ficheros de de los que sea responsable cada entidad. En caso contrario, la utilización de los datos resultaría contraria a lo dispuesto en el artículo 4.2 de la Ley Orgánica 15/1999, a cuyo tenor "los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos"*. Vid., Informe Jurídico AEPD 392/2009, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentación/informes_juridicos /cesion_datos/common/pdfs/2009-0392_Comunicaci-oo-n-de-datos-entre-Organismos-P-uu-blicos.pdf [Consulta 4/07/2015].

[851] La doctrina ha resaltado la vaguedad e imprecisión del precepto pues al referirse a cesiones entre administraciones públicas no concreta que se tenga que realizar a entidades que tengan las mismas competencias, aunque lo lógico sería pensar que así fuera en aras a proteger el cumplimiento del principio de finalidad en el tratamiento de datos. Acerca de este planteamiento vid., LUCAS MURILLO DE LA CUEVA, P.: *Informática y…*,op. cit., pág. 97; VALERO TORRIJOS, J. y LÓPEZ PELLICER J.A.: "Algunas consideraciones sobre el derecho a la protección de datos personales en la actividad administrativa", *Revista Vasca de Administración Pública*, núm. 59, 2001, pág. 283.

[852] Art. 11.2 d) de la LOPD: *"Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas".*

[853] Art. 45.2 de la LOPD: "*2. Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros".*

actuación calificada como grave[854], con la particularidad de que se trata de un organismo público el obligado a cumplir la normativa y, por tanto, la LOPD tiene establecido un procedimiento distintos en estos casos[855].

5.1.2. Características de los ficheros creados en el ámbito de la Administración Pública.

El resultado de todas estas cesiones de datos a la Administración Pública es la configuración de un nuevo fichero, el cual está catalogado como de naturaleza pública[856] y cuya responsabilidad pertenece ahora a los organismos administrativos ya señalados– SEPE, Seguridad Social y Administración Tributaria-. Una vez creado el fichero, estos órganos podrán utilizar esos datos tan sólo para cumplir las funciones determinadas en la normativa y relacionadas con las actuaciones vinculadas a la relación de trabajo, ya que cualquier otro uso iría en contra del principio de calidad.

En relación con el principio de calidad también hay que identificar, en el ámbito de los ficheros públicos, qué sujeto es el obligado a notificar cualquier modificación en la información personal registrada, ahora, en las distintas Administraciones Públicas. En este sentido, cabe decir que el interesado y titular del dato, el trabajador, es el que tendrá que comunicar a la Administración, por ejemplo, un posible cambio en su dirección o la modificación de sus circunstancias personales o familiares para que le ajusten la retención practicada en su nómina. No obstante, lo habitual es que una vez que el trabajador comunica estos cambios al empresario, como encargado de la configuración del recibo de nómina, sea él el que traslade la información a la AEAT a través del modelo 145[857].

---

[854] Art. 44.3 k) de la LOPD: "*La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave".*

[855] Art. 46.1 de la LOPD: " *Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera".*

[856] Vid., pp. 90 y ss del Capítulo primero.

[857] GUICHOT REINA, E.: *Datos personales y…,* op. cit., pp. 226-234; GONZÁLEZ NAVARRO, F.: "La relación jurídica de…", op. cit., pp. 62-63.

Ante el desconocimiento por parte del trabajador de la ubicación de su información personal, debido sobre todo a la cantidad de transferencias de datos que se producen en el inicio de la relación de trabajo, es preciso que el empresario le informe[858] no sólo de la existencia de cesión de datos, sino también de los distintos ficheros que se van a crear con el objetivo de que el trabajador tenga constancia de los sujetos responsables de esos ficheros para así poder ejercer los derechos que la LOPD le confiere[859]. Respecto del consentimiento para tratar los datos incluidos en estos ficheros, se puede aplicar la excepción al consentimiento prevista en el art. 6.2 de la LOPD[860], justificándose en que parece lógica la realización de tareas relacionadas con la gestión del personal, sin que éstas tengan que estar sometidas al arbitrio o voluntariedad del titular del dato[861].

Lógicamente el trabajador podrá ejercer los derechos de acceso, rectificación, cancelación y oposición respecto de los datos contenidos en estos ficheros de la Administración Pública con las mismas garantías que si tuvieran otra naturaleza[862]. Como es sabido, el de acceso de terceros a los ficheros públicos es un derecho reconocido constitucionalmente[863], el cual puede confrontarse con el derecho a la protección de datos de los trabajadores y, por tanto, tendrá que ser limitado ante la posibilidad de que personas ajenas a ese fichero puedan conocer su información personal[864].

Por este motivo, además de lo previsto en la LOPD para el acceso a los datos contenidos en los ficheros y como consecuencia de la configuración

[858] Vid., art. 5.1 de la LOPD.
[859] Derechos de acceso, rectificación, cancelación y oposición.
[860] Art. 6.2 de la LOPD: "*No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias*".
[861] HERRERO DE EGAÑA, J.M.: "Intimidad, tributos y protección de datos personales", *Indret (Revista para el análisis del Derecho)*, núm. 2, 2007, pp.14-16.
[862] Vid., apartado 3.4 del Capítulo primero.
[863] Art. 105 b) de la CE: "*El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas".*
[864] GUICHOT REINA, E.: *Publicidad y privacidad de la información administrativ*a, Thomson-Civitas, 2009, pp. 194-198.

pública de estos ficheros con datos nominativos de los trabajadores[865], es preciso atender a lo establecido, de forma general, en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno[866]. Pero, sobre este aspecto es necesario aclarar que, lógicamente, la información de los trabajadores incluida en esos ficheros no pasa a tener esta catalogación[867], ya que sigue siendo información personal de los mismos, por lo que los términos establecidos en el art. 13 de la Ley 19/2013[868] referidos al acceso a la información pública no son aplicables a estos datos. Tampoco la reciente Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas[869] aporta ninguna novedad al respecto pues hace alusión a lo establecido en la Ley 19/2013, estando está configurada como una ley específica con las particularidades que se pueden dar en el acceso de los ciudadanos a los ficheros públicos.

Por tanto, el criterio de acceso de la Ley 19/2013 difiere de lo contenido en la LOPD, ya que en la misma la conformación y catalogación de estos ficheros como públicos viene dada por la categoría que tengan las entidades que se encargan de su administración y custodia, pero nada dice que los datos allí contenidos tengan esa calificación pública. Por lo que, a pesar de ser ficheros públicos este hecho no convierte a la información registrada en ellos como tal y para su tratamiento la Administración tiene que someterse a lo establecido en la LOPD y respetar los principios de la protección de datos. Por consiguiente, los ficheros cuyos responsables son la Administración de la Seguridad Social, el SEPE y la AEAT son públicos pero tan sólo está permitido el acceso para aquellos sujetos interesados en el expediente[870].

---

[865] Sobre la consideración de información pública de aquellos datos contenidos en los ficheros en poder de las administraciones públicas, véase GUICHOT REINA, E.: T*ransparencia y acceso a la información en el Derecho Europeo*, Ed. Derecho Global, 2011, pp. 105-108.

[866] BOE núm. 295 de 10 de diciembre de 2013.

[867] Véase documento de la AEPD sobre la naturaleza de los ficheros públicos, disponible en https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/naturaleza_ficheros/index-ides-idphp.php [Consulta 26/01/2016].

[868] Art. 13 d) de la Ley 39/2015: *"Al acceso a la información pública, archivos y registros, de acuerdo con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y el resto del Ordenamiento Jurídico".*

[869] BOE núm. 236, de 2 de octubre de 2015, entrada en vigor de la norma el 2 de octubre de 2016 (vid. Disp. Adic. Séptima de la Ley 39/2015).

[870] Art. 5. 1 m) del RDLOPD: *"Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las*

En segundo lugar, desde la entrada en vigor de la Ley 19/2013, para solicitar el acceso no es inexcusable acreditar un interés legítimo en el expediente[871] que se pretende consultar, puesto que en su art. 12[872] no se establece que se tenga que cumplir requisito alguno para solicitar el acceso a los ficheros en los términos previstos legalmente[873]. Aunque sí existen algunas limitaciones descritas en el art. 14 de la Ley 19/2013[874], relacionadas con la posibilidad de que ese acceso pudiera provocar un perjuicio a la seguridad nacional y pública; al secreto profesional; a la política económica y monetaria; a las funciones administrativas inspectoras y de vigilancia; etc.[875].

En tercer lugar, la LOPD nada dice sobre el acceso a los ficheros con datos de carácter personal que pudiera efectuar un tercero, refiriéndose únicamente al posible conocimiento de estos datos por otra persona si lo que se pretende con este acceso es prestar un servicio al responsable del tratamiento[876]. Por ello, hay que acudir de nuevo a lo establecido en la Ley 19/2013 que regula el acceso a los documentos en poder de las distintas

---

instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público".

[871] Sobre este aspecto la jurisprudencia ha establecido la posibilidad de que otros ciudadanos, distintos al interesado, pueda conocer la información personal contenida en esos expedientes, vid., Sentencia del Tribunal Supremo de 16 de diciembre de 2011 (RJ 2012\2832), en la que se resuelve que esos terceros interesados en el expediente tendrán que acreditar un interés legítimo y directo para acceder. Sin embargo a partir de la modificación del art. 37 de la Ley 30/1992, la cual remite lo relacionado con el acceso a la Ley 19/2013, no se hace preciso probar un interés legítimo en el expediente para solicitar el conocimiento de os datos allí contenidos.

[872] Art. 12 de la Ley 19/2013: *"Todas las personas tienen derecho a acceder a la información pública, en los términos previstos en el artículo 105.b) de la Constitución Española, desarrollados por esta Ley. Asimismo, y en el ámbito de sus respectivas competencias, será de aplicación la correspondiente normativa autonómica".*

[873] En conexión con lo establecido en el art. 12 de la Ley 19/2013, véase lo previsto en el art. 17.3 respecto a la no necesidad de motivar la solicitud de acceso: *"El solicitante no está obligado a motivar su solicitud de acceso a la información. Sin embargo, podrá exponer los motivos por los que solicita la información y que podrán ser tenidos en cuenta cuando se dicte la resolución. No obstante, la ausencia de motivación no será por si sola causa de rechazo de la solicitud".*

[874] Vid., art. 14 de la Ley 19/2013.

[875] Acerca del acceso a la información pública vid., el interesante análisis realizado por TRONCOSO REIGADA, A. del art. 37 de la Ley 30/1992 antes de la publicación de la Ley 19/2013, en *Transparencia administrativa y protección de datos de carácter personal*, Civitas, 2008, pp. 32-34; y en el mismo sentido RAZQUIN LIZARRAGA, M.: *La confidencialidad de los datos empresariales en poder de las Administraciones Públicas*, Iustel, 2013, pp. 107-113; VV.AA.: *Transparencia, acceso a la información pública y buen gobierno: Estudio de la Ley 19/2013, de 9 de diciembre,* Tecnos, 2014, pp.199-220.

[876] Vid., art. 12 de la LOPD.

Administraciones Públicas, la cual sí tiene previsto en su art. 15[877] exigencias para garantizar el derecho a la protección de datos, pudiendo deducirse de su contenido que, para acceder a los datos, no se tiene que por qué recabar el consentimiento del titular de los datos, tan sólo debiendo mediar ese asentimiento, además expreso y por escrito, si esos datos contenidos en los ficheros fueran especialmente sensibles. Aunque ese acceso no exija el consentimiento del titular, será el órgano administrativo correspondiente el que admita o no la solicitud de acceso a tenor de lo establecido en el art. 15.3 de la Ley 19/2013[878] en el que se expone que el acceso se concederá previa ponderación suficientemente razonada del interés público frente al derecho a la protección de los datos.

Por otra parte, existe un sector doctrinal que considera este acceso a los datos por parte de un tercero como una cesión o comunicación de datos[879],

[877] Art. 15.1 de la LOPD: *"1. Si la información solicitada contuviera datos especialmente protegidos a los que se refiere el apartado 2 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso. Si la información incluyese datos especialmente protegidos a los que se refiere el apartado 3 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, o datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso sólo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquél estuviera amparado por una norma con rango de Ley. 2. Con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano".*

[878] Art. 15.3 de la Ley 19/2013: *"3. Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal. Para la realización de la citada ponderación, dicho órgano tomará particularmente en consideración los siguientes criterios: a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos. c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos. d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en* el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad".

[879] En este sentido véase, PIÑAR MAÑAS, J.L.: "Transparencia y protección de datos. Una referencia a la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno" en VV.AA.: *Transparencia, acceso a la información y protección de datos*, Reus, 2014, pp.59-62.

aplicándose lo establecido en la LOPD[880] para estos supuestos. Así pues, si el acceso se considerara cesión de datos, podrá prescindirse del consentimiento del titular teniendo en cuenta lo contenido en el art. 11. 2 a) de la LOPD, ya que la Ley 19/2013 supone el título habilitante para poder llevar a cabo la comunicación sin la autorización del titular del dato. En este sentido, evidentemente, se podría considerar cesión de datos, puesto que se puede presumir que la concesión del acceso al expediente administrativo por parte de los órganos administrativos competentes conlleva no sólo la visualización de los datos de carácter personal, sino también el archivo o registro de esos datos por ese tercero[881], no diferenciándose, entonces, de otras comunicaciones de datos que se puedan realizar.

5.2. Cesiones de datos a los representantes de los trabajadores.

5.2.1. Cesiones de datos a los representantes unitarios.

Con carácter general, las informaciones que el empresario tiene que dar a los representantes de los trabajadores en la empresa pueden ser consideradas como informaciones genéricas que no identifican claramente a ningún trabajador[882]; y, de ser esto así, no se trataría de datos que comprometan el derecho a la protección de datos de carácter personal. Sin

[880] Vid., art. 11 de la LOPD.

[881] Art. 15.5 de la Ley 19/2013: *"La normativa de protección de datos personales será de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso"*.

[882] Recomendación 1/2006 de la Agencia de Protección de Datos de la Comunidad de Madrid sobre cesiones de datos de los empleados públicos de dicha Comunidad a las Secciones sindicales, Comités de Empresa y Juntas de Personal; "*A la vista de las previsiones legales que habilitan las funciones y competencias de las secciones sindicales, comités de empresa y juntas de personal que han sido detalladas en el apartado anterior, se considera que, de acuerdo con la Ley Orgánica de Protección de Datos de Carácter Personal, dichas previsiones no especifican con carácter general que se tenga que proceder a la cesión de datos personales de los empleados públicos en los siguientes supuestos: Para conocer el establecimiento de la jornada laboral y horario de trabajo, régimen de permisos, vacaciones y licencias; emitir informe sobre materias como traslado total o parcial de las instalaciones, planes de formación de personal o implantación o revisión de sistemas de organización y método de trabajo; conocer las estadísticas sobre el índice de absentismo y sus causas, los accidentes en acto de servicio y enfermedades profesionales y sus consecuencias, los índices de siniestralidad, los estudios periódicos o especiales del ambiente y las condiciones de trabajo, así como las correspondientes a recibir información trimestral sobre política de personal. En consecuencia, estas funciones, en principio, tienen que desarrollarse sin necesidad de proceder a una cesión total y completa de los datos personales de los empleados públicos, salvo que hubieran dado su consentimiento, y ello derivado de que, con carácter general, dicha cesión de datos no está contemplada específicamente ni en el Estatuto de los Trabajadores, ni en la Ley 9/1987, de 12 de junio, de Órganos de Representación, Determinación de las Condiciones de Trabajo y Participación del Personal al Servicio de las Administraciones Públicas."*

embargo, en algunos supuestos particulares parece que los representantes de los trabajadores si que tienen conocimiento de algunos datos personales de los trabajadores, por lo que habrá que valorar en que situaciones se trata de una información que está, o no, excluida del ámbito de aplicación de la LOPD.

Una de las primeras notificaciones realizada por el empresario es la comunicación de la copia básica del contrato de trabajo a los representantes de los trabajadores en la empresa. Esta actuación se configura como una obligación empresarial para cumplir con lo establecido en el art. 8.4 del ET[883]. Tal comunicación de la copia básica del contrato de trabajo se puede efectuar sin que medie el consentimiento del trabajador, ya que es una actuación prevista en la normativa laboral, materializándose, entonces, la excepción al consentimiento prevista en el art. 11.2 a) de la LOPD[884]. Ahora bien, esta excepción no opera en principio sobre todos los datos del contrato de trabajo ya que el propio art. 8.4 del ET establece que los datos cedidos a los representantes de los trabajadores sólo serán aquellos que no colisionen con su derecho a la intimidad excluyendo de la citada cesión; el domicilio; DNI; estado civil; etc.[885]siguiendo lo expuesto en el art. 11.1 de la Ley 2/1991, de 7 de enero, sobre información a los representantes de los trabajadores en materia de contratación[886].

[883] Art. 8.4 del ET: "*El empresario entregará a la representación legal de los trabajadores una copia básica de todos los contratos que deban celebrarse por escrito, a excepción de los contratos de relación laboral especial de alta dirección sobre los que se establece el deber de notificación a la representación legal de los trabajadores".*

[884] Sobre este asunto vid., Informe Jurídico 488/2009 de la AEPD, disponible en http:// www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesiondatos/common/pdfs/2009-0488_Cesi-oo-n-de-datos-de-trabajadores-a-comit-ee--de-empresa.-Ley-habilitante.-Alcance.pdf; Informe Jurídico 384/2010 de la AEPD, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2010-0384_Cesi-oo-n-a-comit-ee--de-empresa-de-datos-de-trabajadores-prevista-en-convenio.-Oposici-oo-n-por-alg-uu-n-trabajador.pdf [Consulta 4/07/2015].

[885]Art. 8.4 del ET: *"Con el fin de comprobar la adecuación del contenido del contrato a la legalidad vigente, esta copia básica contendrá todos los datos del contrato a excepción del número del documento nacional de identidad o del número de identidad de extranjero, el domicilio, el estado civil, y cualquier otro que, de acuerdo con la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, pudiera afectar a la intimidad personal".*

[886] BOE núm. 7 de 8 de enero de 1991.

También existe la posibilidad de ceder a los representantes de los trabajadores los datos salariales de los empleados[887], lo que ha propiciado algunos pronunciamientos jurisprudenciales contradictorios. De una parte, siguiendo la doctrina constitucional establecida por la Sentencia de 22 de abril de 1993[888], se considera que la comunicación de los datos retributivos del trabajador no viola derecho constitucional alguno[889]; no obstante, hay un sector jurisprudencial contrario a esta cesión, especificando que estos representantes no tienen por qué conocer este dato del trabajador y que no es

[887] La normativa laboral no expone claramente que el comité de empresa tenga que ser informado acerca del salario de los trabajadores pero esta comunicación de datos se deduce del contenido del contrato de trabajo y de su no inclusión en los datos precisos para comprobar la adecuación del contrato de trabajo.

[888] Sentencia del Tribunal Constitucional de 22 de abril de 1993 (RTC 1993/142); "*Las retribuciones que el trabajador obtiene de su trabajo no pueden en principio desgajarse de la esfera de las relaciones sociales y profesionales que el trabajador desarrolla fuera de su ámbito personal e íntimo, para introducirse en este último , y hay que descartar que el conocimiento de la retribución percibida permita reconstruir la vida íntima de los trabajadores. Al margen de que la Ley 2/1991 se limita a imponer la obligación de incluir en la «copia básica» la retribución pactada en un único momento de la relación laboral -el de su inicio, pues las sucesivas modificaciones sólo son objeto de notificación (1.2 Ley 2/1991)-, lo cierto es que el acceso a la información relativa a la retribución no permite en modo alguno la reconstrucción de datos del trabajador incluidos en la esfera de su intimidad . En este sentido, no puede olvidarse que, por sí solo, el dato de la cuantía retributiva, aparte de indicar la potencialidad de gasto del trabajador, nada permite deducir respecto a las actividades que, sólo o en compañía de su familia, pueda desarrollar en su tiempo libre. No es ocioso recordar que aún antes de la Ley 2/1991 los salarios percibidos eran ya accesibles al conocimiento de los representantes de los trabajadores, en cuanto tales salarios sirven de base de cotización a la Seguridad Social, y dichos representantes pueden conocer y comprobar los correspondientes documentos de cotización [art. 87.3, Orden de 23 de octubre de 1986 (RCL 1986\3324 y RCL 1987\531), y art. 95.3, Orden de 8 de abril de 1992 (RCL 1992\903)]."*

[889] En un principio se podría considerar este dato como ajeno a lo que configura la copia básica del contrato de trabajo, pero la jurisprudencia ha estimado su inclusión justificando la misma en la necesidad de conocer estos datos para ver si se ajustan a lo establecido en el Convenio colectivo. Así, la Sentencia del Tribunal Supremo de 9 de febrero de 2009 (RJ 2009\1620) establece; ", *la retribución o salario no es un dato de carácter personal ni íntimo susceptible de reserva para salvaguardar el respeto a la intimidad. Se trata de un elemento esencial del contrato de trabajo, de naturaleza contractual, laboral y profesional, no siendo necesario recabar el consentimiento previo del trabajador individual para que los representantes sindicales puedan acceder, en su caso, a dicho dato. Ahora bien, estas consideraciones no implican el éxito del recurso, en cuanto está aquí acreditado que la empresa demandada ha entregado la copia básica de los contratos y ha facilitado la información de los salarios por categorías y departamentos, información que cumple suficientemente con las exigencias que al respecto establece el artículo 1 de la Ley 2/1991 (RCL 1991, 39) , de enero, que regula los derechos de información de los trabajadores en materia de contratación, en cuanto dispone este precepto que "con el fin de comprobar la adecuación del contenido del contrato a la legalidad vigente, esta copia básica contendrá todos los datos del contrato a excepción del número del DNI, el domicilio, el estado civil y cualquier otro que, de acuerdo con la Ley Orgánica 1/1982, de 5 mayo (RCL 1982, 1997) , pudiera afectar a la intimidad personal", sin que el convenio colectivo de empresa aplicable amplíe en esta materia los derechos establecidos en dicha Ley, y sin que el Sindicato demandante haya expuesto algún tipo de concreta justificación, que hiciera necesario el conocimiento de los datos solicitados en relación con el ejercicio de las funciones que constitucionalmente tiene reconocidas"*

necesaria su comunicación para que éstos puedan realizar sus funciones, como así ha dictaminado también la AEPD, respecto de determinados complementos retributivos de los empleados públicos[890].

En todo caso, ha de entenderse que la comunicación del dato relativo a las retribuciones del trabajador no constituye un atentado contra la intimidad del trabajador y contra su derecho a la protección de datos de carácter personal[891], si se realiza con la finalidad de permitir comprobar que esos datos del trabajador son respetuosos de las garantías legales y convencionales, y para permitir que, en el caso de que no sea así, los representantes de los trabajadores pudieran ejercer las acciones pertinentes ante la Administración Laboral[892]. Esta sería, por tanto, la finalidad legítima de la cesión de la copia básica del contrato para no incurrir en una posible vulneración del derecho a la protección de datos de carácter personal, pues la comunicación del dato para cualquier otro fin precisaría el consentimiento del trabajador[893].

---

[890] Según la AEPD; *"A la vista de todo lo que se ha venido indicando cabe concluir, modificando el criterio hasta ahora sustentado por esta Agencia, que la cesión a los representantes sindicales de los datos referidos a las percepciones individualizadas por los empleados públicos en concepto de complemento de productividad y gratificaciones no se encuentra amparada por el artículo 11.1 a) de la Ley Orgánica 15/1999, siendo preciso para que dicha cesión de datos pueda tener lugar el consentimiento de los afectados. En consecuencia, y como se fundamenta en el informe antes expuesto, no se permite la cesión a los representantes sindicales de los datos referidos a la productividad de los empleados públicos, dado que dicha cesión no se encuentra amparada en el artículo 11.2 a) de la Ley Orgánica 15/1999 pudiendo sólo conocer los criterios que se han tenido en cuenta en relación con los puestos de trabajo para conceder o no la productividad*", en Informe Jurídico 275/2009 de la AEPD, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2009-0275_Determinaci-oo-n-del-tipo-de-informaci-oo-n-que-se-comunica-a-las-juntas-de-personal-y-delegado-sindical.pdf [Consulta 20/08/2015]

[891] APILLUELO MARTIN, M.: "Derecho de información del delegado sindical a las retribuciones de los trabajadores y derechos a la libertad sindical y a la protección de datos de carácter personal" *Revista Doctrinal Aranzadi Social*, núm. 28, 2011.pp.1-5; RABANAL CARBAJO, P.: "Derechos de información de los representantes de los trabajadores. Condiciones económicas precisas de los contratos. Deben comunicarse aun en contra de la voluntad de los trabajadores afectados", *Aranzadi Social*, núm. 14, 2006 pp.1-2.

[892] MONEREO PÉREZ, J.L.: *Los derechos de información de los representantes de los trabajadores*, Madrid (Civitas), 1992, pág. 463; SAGARDOY BENGOECHEA, J.A. Y GIL Y GIL, J.L.: "Derechos de información de los representantes de los trabajadores en materia de contratación", *Revista de Trabajo*, núm. 100, 1990, pág. 31; TASCÓN LÓPEZ, R.: "El tratamiento por los representantes de los trabajadores y por las organizaciones sindicales de los datos personales de los trabajadores: entre lo fácticamente posible, lo socialmente conveniente y lo jurídicamente aceptable" *Revista Española de Protección de datos*, núm.1, 2006, pp. 215-220.

[893] BARBANCHO TOVILLAS, F.: "Derecho a la información sobre retribuciones de sección sindical versus derecho a la intimidad y protección de datos personales en la Sociedad Estatal de Correos", *Aranzadi Social*, núm. 30, 2007.pp.4-8.

Otro de los casos que pueden resultar conflictivos, en cuanto a la cesión de datos a los representantes de los trabajadores, puede ser el relacionado con las peticiones de censos electorales formuladas por las centrales sindicales para la campaña de elecciones sindicales. Para lo que es preciso establecer si para estas comunicaciones de datos es necesario el consentimiento expreso del trabajador o puede obviarse. Es cierto que la representación de los trabajadores en la empresa no necesita acudir al censo para obtener datos de los trabajadores puesto que accede a ellos a través de la copia básica del contrato. Lo que ocurre es que, ya que estas informaciones del trabajador no podrán ser utilizadas sin su consentimiento para finalidades distintas de las previstas, las cedidas en la copia básica del contrato no podrán usarse para llevar a cabo, por ejemplo, envío de propaganda electoral a los trabajadores, pues se estaría vulnerando con esta acción el principio de calidad de los datos.

A este respecto, existe una habilitación legal para que la empresa tan sólo deba entregar el censo electoral a las mesas electorales[894] constituidas al efecto, siendo éstas las encargadas de darles publicidad entre los trabajadores[895]. En ocasiones, puede que el envío se realice directamente de la empresa a los sindicatos como consecuencia de un acuerdo colectivo. En estos supuestos la jurisprudencia[896] ha hecho una interpretación flexible de la

[894] Art. 74.2 y 3 del ET: "*2. Cuando se trate de elecciones a delegados de personal, el empresario, en el mismo término, remitirá a los componentes de la mesa electoral el censo laboral que se ajustará, a estos efectos, a modelo normalizado. 3. Cuando se trate de elecciones a miembros del comité de empresa, constituida la mesa electoral solicitará al empresario el censo laboral y confeccionará, con los medios que le habrá de facilitar éste, la lista de electores. Esta se hará pública en los tablones de anuncios mediante su exposición durante un tiempo no inferior a setenta y dos horas".*

[895] TRONCOSO REIGADO, A.: *La protección de datos*…, op. cit., pp.1583-1585; RODRÍGUEZ RAMOS, M.J.: *Las elecciones sindicales en la empresa y en los centros de trabajo*, Aranzadi, 2002, pp. 262-265.

[896] Sentencia del Tribunal Supremo de 27 de septiembre de 2007 (RJ 2007\7095); " *Y analizando los recursos entablados, es evidente que la sentencia impugnada no vulnera el artículo 74.3 del Estatuto (RCL 1995, 997) ni lo interpreta erróneamente porque aunque dicho precepto, igual que la mayoría de las normas de la Sección 2ª ("Procedimiento electoral") del Capítulo I de su Título II, como acertadamente sostiene la Sala de instancia, constituye una clara previsión de derecho necesario, ello no supone que su contenido mínimo no pueda ser mejorado por la negociación colectiva en aras de mayores garantías y de una mejor y más completa participación de todos los sujetos implicados, que participen o aspiren a participar, en la elección de representantes unitarios de los trabajadores, en especial de los entes sindicales con implantación o presencia en el seno de la empresa, máxime si reparamos en que, como pone de relieve el escrito de impugnación de CCOO, la dispersión y el alto número de centros de trabajo que se dan en el sector de las entidades de ahorro y el reducido número de trabajadores destinados en cada uno de ellos, entre otras circunstancias, podría haber sido la*

norma, permitiendo esta comunicación sin que medie el consentimiento expreso del trabajador, puesto que no se estaría vulnerando las exigencias de la normativa laboral para el traslado del censo a la mesa electoral, sino que se estaría procurando, a través de un acuerdo colectivo, que esta información llegue a más sujetos implicados en las elecciones como es el caso de los propios representantes de los trabajadores. Así pues, esta actuación no tiene por qué estar legitimada por el consentimiento expreso del trabajador, pues lo que se pretende es facilitar la actividad de los representantes de los trabajadores en un momento concreto como puede ser el desarrollo de la campaña electoral en las elecciones sindicales[897].

En el ámbito de la salud laboral también existen previsiones legales que autorizan la cesión de datos, con información médica de los trabajadores, a los representantes unitarios de los mismos[898]. Estos datos versaran mayoritariamente sobre los accidentes de trabajo acaecidos en la empresa con identificación del trabajador que lo haya padecido. Por este motivo, al tratarse de un dato especialmente protegido la LOPD, permite su comunicación, como es sabido, cuando exista consentimiento expreso del interesado o cuando exista una habilitación legal que así lo determine. En este sentido la LPRL[899]

---

principal razón por la que se pactó la entrega de los censos para que los sindicatos pudieran ejercer su labor de preparación de las candidaturas e incluso controlar el correcto contenido del propio censo. …En efecto, como la sentencia recurrida sostiene, si la totalidad de los datos profesionales y personales que contienen los censos laboral y electoral de la empresa demandada, recogidos en el núm. 2 de su hecho probado sexto, son objeto de la publicidad prevista y ordenada legalmente en el artículo 74.3 del Estatuto -lo que, sin perjuicio de la persecución de aquellas conductas concretas que pudieran sobrepasar los límites de las referidas leyes orgánicas, elimina la necesidad de solicitar y obtener un consentimiento personal específico como medio alternativo al contemplado en dichas normas-, es claro que no se produce la conculcación del artículo 18.1 CE y de la citada legalidad orgánica por el simple hecho de que a tal publicidad se le pueda añadir otra complementaria, dirigida a determinadas entidades o agrupaciones, y con la exclusiva finalidad de facilitar su natural actividad sindical dentro de un muy concreto proceso electoral a representantes unitarios de los trabajadores, sobre todo cuando, como antes de dijo, la mejora que constituye esa extensión de la publicidad es el producto de un pacto colectivo del que sin duda se beneficia también el sindicato demandante y que no consta impugnado en forma alguna."

[897] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos*…, op. cit., pp. 266-269.

[898] Art. 64. 2 d) del ET: *"De las estadísticas sobre el índice de absentismo y las causas, los accidentes de trabajo y enfermedades profesionales y sus consecuencias, los índices de siniestralidad, los estudios periódicos o especiales del medio ambiente laboral y los mecanismos de prevención que se utilicen".*

[899] Art. 39.2 c) de la LPRL: *"2. En el ejercicio de sus competencias, el Comité de Seguridad y Salud estará facultado para: c) Conocer y analizar los daños producidos en la salud o en la*

faculta a los delegados de prevención incluidos en los Comités de Seguridad y Salud, para conocer un listado de trabajadores en el que se incluya nombre y apellidos del trabajador, fecha del accidente laboral, tipo de lesión y forma en que se produjo, así como, la fecha de alta y baja laboral.

Por otra parte, según lo establecido en la normativa laboral, el comité de empresa tiene derecho a conocer el nivel de absentismo laboral[900]de forma genérica, es decir, sin referencias concretas a ningún trabajador de la empresa y sólo con la intención de elaborar los estudios y estadísticas sobre el absentismo y sus causas. El conocimiento de esta información por parte del Comité de Empresa no se considera cesión de datos, puesto que los datos son generales y disociados, no distinguiéndose ningún empleado de la empresa. Así pues, esa información sólo sirve para realizar listados de absentismo de forma global, sin dar datos personales de los trabajadores implicados y sin que el Comité de Empresa pueda exigir esta información en ningún momento. A pesar de esto, la LOPD ha previsto una excepción al consentimiento del trabajador si los datos son previamente disociados y esa comunicación a un tercero es sólo para establecer estadísticas puntuales no identificativas[901].

5.2.2. Cesiones de datos del empresario al sindicato.

Parece evidente que el empresario tiene que ceder datos de sus empleados a los sindicatos para que éstos puedan realizar las funciones de representantes sindicales[902]. En tal caso está cesión se podrá realizar sin el consentimiento del titular de los datos al venir autorizada por una Ley –art. 11 a) de la LOPD-. Aunque sólo podrán tratar estos datos en la medida en que

---

integridad física de los trabajadores, al objeto de valorar sus causas y proponer las medidas preventivas oportunas".

[900] Art. 64.2.d) del ET: *"El comité de empresa tendrá derecho a ser informado trimestralmente: d) De las estadísticas sobre el índice de absentismo y las causas, los accidentes de trabajo y enfermedades profesionales y sus consecuencias, los índices de siniestralidad, los estudios periódicos o especiales del medio ambiente laboral y los mecanismos de prevención que se utilicen".*

[901] Art. 11.6 de la LOPD:*"Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores."*

[902] Título IV de la LOLS.

sean necesarios y pertinentes para el cumplimiento de sus funciones sindicales[903].

Por este motivo, el empresario podría negarse a dar información de sus trabajadores al sindicato si ésta no es precisa para que éste desarrolle su actividad sindical, puesto que para que esa comunicación de datos, de naturaleza adicional a los estrictamente necesarios, sea respetuosa con las exigencias legales, se requiere el consentimiento ese trabajador[904]. Una vez que se ha cedido el dato mediante habilitación legal o con el consentimiento del afiliado, el sindicato tendrá que utilizar los datos siguiendo el principio de calidad, es decir, usando esa información de acuerdo con la finalidad que propició su recogida.

Teniendo en cuenta que la cesión de esos datos, autorizada por la Ley, se ha dado sin el consentimiento del trabajador, la representación sindical tendrá que informar a esos trabajadores del tratamiento que le van a dar a sus datos profesionales y de la existencia de ese fichero. Esta información tiene relevancia ya que los trabajadores normalmente no tienen constancia del traspaso de esos datos y de su posible registro en un fichero sindical, por lo que es muy importante que se informe de estas circunstancias para que así puedan ejercer los derechos que la LOPD les confiere como titulares de datos de carácter personal. Actualmente, esta obligación de informar no puede quedar eximida siguiendo el criterio del art. 5.5 de la LOPD (que establece que se puede exceptuar esta obligación si la misma exige un esfuerzo desproporcionado), pues con la implantación de las TICs parece difícil pensar que no se pueda transmitir estas advertencias haciendo uso de los canales de

[903] El Tribunal Constitucional en su Auto 29/2008, de 28 de enero (RTC 2008\29), ha considerado que la cesión de datos profesionales de los trabajadores a los sindicatos sólo se permite para realizar una acción concreta relacionada con la actividad sindical en este caso.

[904] Así, la jurisprudencia ha estimado como lícita la negativa empresarial a dar al sindicato algunas informaciones acerca de aspectos del trabajador que no sean necesarios para cumplir con sus finalidades sindicales como las direcciones particulares de los trabajadores de ayuda a domicilio (Sentencia del TSJ de Andalucía de 18 de julio de 2007 (AS 2008\174)). Sin embargo, ha establecido vulneración del ejercicio de la actividad sindical en aquellos casos en los que la empresa no aporta información a los representantes sindicales sobre trienios, suplencias, horas extras etc. de los trabajadores (Sentencia del TSJ del País Vasco de 16 de mayo de 2006 (AS 2007\1028) y del TSJ de Cataluña de 18 de enero de 2010 (AS 2010\983)).

comunicación que las mismas proporcionan –correo electrónico o mecanismos similares-[905].

5.2.3. Las cesiones de datos del sindicato a la empresa.

En cuanto a las cesiones de datos de afiliados realizadas por los sindicatos al empresario también tienen que mediar las suficientes garantías para cumplir con lo establecido en la normativa sobre protección de datos. En primer lugar, y como regla general, la organización sindical tiene que contar con el consentimiento expreso del trabajador afiliado[906], que debe otorgase de forma escrita, para ceder ese dato a la empresa; en segundo lugar, este afiliado debe conocer el objetivo de la cesión de su dato de afiliación, así como la posibilidad de que sea incluido en un fichero empresarial; y, por último, se debe informar al trabajador sobre los usos que se le van a dar a sus datos, así como de los mecanismos que la LOPD le otorga para acceder, rectificar, cancelar y oponerse a la continuidad de esos datos en el fichero empresarial[907].

El empresario debe utilizar esta información cedida por el sindicato, como es obligado, con la única intención de realizar el descuento en la nómina de ese trabajador de la cuota sindical, a tenor de lo establecido en el art. 11.2 de la LOLS[908], por lo que cualquier utilización que no se limite a esta minoración de la cuota sindical irá en contra del principio de calidad establecido para el tratamiento de información personal.

La exclusividad restrictiva en el uso del dato de afiliación de los trabajadores a la finalidad de recaudación de la cuota sindical, hace que su uso para otras finalidades debe considerarse ilegítimo. Así lo resolvió la Sentencia del Tribunal Constitucional de 13 de enero de 1988 abordando un caso de

[905] Sobre estos aspectos véase el interesante análisis realizado por RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos…,* op. cit., pp. 240-242.
[906] Vid., art. 7 de la LOPD.
[907] TASCÓN LÓPEZ, R.: "El tratamiento por los representantes de los trabajadores y…", op. cit., pág. 214; TRONCOSO REIGADA, A.: "Libertad sindical, libertad de empresa y autodeterminación informativa de los trabajadores", en FARRIOLS I SOLA, A. (COORD.): *La protección de datos de carácter…,* op. cit.,pp. 114 y ss.
[908] Art. 11.2 de la LOLS: *"El empresario procederá al descuento de la cuota sindical sobre los salarios y a la correspondiente transferencia a solicitud del sindicato del trabajador afiliado y previa conformidad, siempre, de éste".*

descuento en nómina de los participantes en una huelga para lo que el empresario había hecho uso de la información sindical sobre afiliación obtenida a los exclusivos efectos del descuento de la cuota. Considerando con esta minoración de la nómina del trabajador se estaba incumpliendo con el cometido principal de la recogida del dato y, a su vez, contradiciendo el principio de información, puesto que el trabajador consintió el tratamiento de sus datos sindicales atendiendo a la información dada por el empresario sobre su utilización –descuento de la cuota sindical-[909]. De forma que la retención de haberes para otros fines distintos e incompatibles con los consentidos por el trabajador lesiona el derecho a la protección de datos pues, en ningún momento, esa cesión de datos relativos a la afiliación sindical se debe utilizar para aplicar el descuento de los días de huelga en el sueldo del trabajador[910].

En otro orden de cosas, hay que considerar si el empresario puede recibir y registrar información acerca de la afiliación de sus trabajadores , con la única finalidad de reducir el crédito horario que tengan la condición de

[909] Sentencia del Tribunal Constitucional de 13 de enero de 1998 (RJ 11/1998); *"Partiendo de estas premisas, en este caso debe tenerse en consideración que la afiliación del trabajador recurrente a determinado Sindicato, se facilitó con la única y exclusiva finalidad lícita de que la Empresa descontara de la retribución la cuota sindical y la transfiriera al Sindicato, de acuerdo con lo establecido en el art. 11.2 LOLS. Sin embargo, el dato fue objeto de tratamiento automatizado y se hizo uso de la correspondiente clave informática para un propósito radicalmente distinto: retener la parte proporcional del salario relativa al período de huelga. Es más, aunque el responsable de la dependencia donde el recurrente presta servicios había participado que éste no se adhirió a la huelga, la Empresa procedió a la detracción sin llevar a cabo investigación alguna en punto a si el demandante efectivamente se sumó a los paros; simplemente presumió que ello fue así por el simple hecho de pertenecer a uno de los Sindicatos convocantes de la huelga, como viene a reconocer su representación procesal en las alegaciones vertidas en este proceso y lo corrobora la circunstancia de que tan sólo el 1 por 100 de los errores afectara a trabajadores afiliados a otros sindicatos o sin militancia sindical conocida. En suma, ha de concluirse que tuvo lugar una lesión del art. 28.1 en conexión con el art. 18.4 CE. Este no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, como ha quedado dicho, sino que además, consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la privacidad según la expresión utilizada en la Exposición de Motivos de la Ley Orgánica reguladora del Tratamiento Automatizado de Datos de Carácter Personal- pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la informatización de los datos personales propicie comportamientos discriminatorios. Y aquí se utilizó un dato sensible, que había sido proporcionado con una determinada finalidad, para otra radicalmente distinta con menoscabo del legítimo ejercicio del derecho de libertad sindical".*

[910] En este mismo sentido véase; Sentencia del Tribunal Constitucional de 15 de junio de 1998 (RTC 1998\123); Sentencia del Tribunal Constitucional de 13 de julio (RTC 1998\158), Sentencia del Tribunal Constitucional de 18 de mayo (RTC 1998\105); Sentencia de la Audiencia Nacional de 27 de mayo de 2004 (AS 2004/2726).

liberados sindicales[911] por pertenecer a una sección sindical con presencia en el centro de trabajo[912]. Este conocimiento de la lista nominal de afiliados a un sindicato no puede vulnerar el derecho a la libertad sindical, mucho menos si esa información puede venir impuesta por el convenio colectivo[913]. A estos efectos, el empresario podría tratar ese dato de afiliación sindical sin que mediara el consentimiento de ese trabajador afiliado, basando su ausencia en la habilitación legal del art. 68 e) del ET, pero no podrá utilizar ese dato para cualquier otra acción que no sea descontar el crédito horario acordado para la realización de su tarea sindical. De esta forma cumple con el principio de finalidad de los datos, preservando siempre que se tendrá que solicitar el consentimiento del titular del dato cuando se prevea su uso para otros fines[914].

---

[911] Como es sabido la condición de liberado sindical se adquiere por la acumulación de todas las horas retribuidas a la representación de trabajadores en sólo uno de ellos, a tenor de lo establecido en el art. 68 e) ET; "*Disponer de un crédito de horas mensuales retribuidas cada uno de los miembros del comité o delegado de personal en cada centro de trabajo, para el ejercicio de sus funciones de representación, de acuerdo con la siguiente escala: 1.Hasta cien trabajadores, quince horas. 2 De ciento uno a doscientos cincuenta trabajadores, veinte horas. 3. De doscientos cincuenta y uno a quinientos trabajadores, treinta horas. 4. De quinientos uno a setecientos cincuenta trabajadores, treinta y cinco horas. 5. De setecientos cincuenta y uno en adelante, cuarenta horas"*.

[912] BALLESTER PASTOR, I.: "Sobre la expansión sostenida de la garantía de indemnidad retributiva del liberado sindical" Aranzadi Social, núm. 13, 2010, pp.1-3; BENÍTEZ-DONOSO LOZANO, J.: "Sobre el reconocimiento de los derechos profesionales de los liberados sindicales: a propósito de la sentencia del Tribunal Constitucional 90/2008 de 21 de julio" *Revista de Derecho Social,* núm. 44, 2008, pp.147-149; GARCÍA NINET, J.I.: "Derecho a la indemnidad económica y profesional: del liberado sindical y promoción laboral. Breves cuñas en torno a la STC 90/2008, de la Sala Primera, de 21 de julio", *Tribuna Social: Revista de Seguridad Social y laboral*, núm. 215, 2008, pp. 5-11; FUENTES RODRÍGUEZ, F.: "Contenido de la libertad sindical: Compatibilidad de la condición de liberado sindical con la ocupación de una plaza en situación especial en activo" *Temas Laborales*, núm. 55, 2000, pp. 217-221; RODRÍGUEZ-PIÑERO ROYO Y DE SOTO RIOJA, S.: "Comentario al art. 11 de la LOLS" en VV.AA.: *La Ley Orgánica de Libertad Sindical. Comentada y con jurisprudencia*, La Ley, 2010, pp. 634-639.

[913] Sentencia del Tribunal Supremo de 8 de abril de 2014 (RJ 2014\4346); "*En suma, ha de concluirse que tuvo lugar una lesión del art. 28.1 en conexión con el art.18.4 C .E. Éste no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, como ha quedado dicho, sino que además, consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la privacidad según la expresión utilizada en la Exposición de Motivos de la Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de Carácter Personal, pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la informatización de los datos personales propicie comportamientos discriminatorios. Y aquí se utilizó un dato sensible, que había sido proporcionado con una determinada finalidad, para otra radicalmente distinta con menoscabo del legítimo ejercicio del derecho de libertad sindical. La empresa recurrente aportó a los autos unos listados con información sensible, sin estar autorizada a ello, y que disponía de los mismos con otra finalidad bien distinta a la que intentó hacerlos valer, por lo que acierta la sentencia de instancia en acordar su inadmisión al ser innecesarios para la resolución que se le planteó, y a la vez, sin lugar a dudas vulneradores de derechos fundamentales".*

[914] Hay supuestos en los que se le descuentan conceptos retributivos de la nómina por el simple hecho de ser liberado sindical, extralimitándose el empresario con esta acción en el uso

5.3. Las distintas comunicaciones de datos médicos en las relaciones de trabajo.

Como se sabe, entre las obligaciones preventivas de la empresa se encuentra la de conservar la documentación [915] relativa a los accidentes de trabajo que se hayan producido en su empresa y a la práctica de los controles de estado de salud de los trabajadores en virtud de lo establecido en al art. 23.1 de la LPRL[916], debiendo ceder esos datos relativos a la salud de los trabajadores a la Autoridad Laboral y a otros trabajadores cuyas tareas estén relacionadas con las actividades preventivas[917]; para, de esta forma, cumplir con sus obligaciones en materia de prevención de riesgos laborales. Estos datos no son reveladores de circunstancias personales sobre el estado de salud de los trabajadores, ya que recogen información sobre conclusiones de los reconocimientos médicos y otras de carácter general acerca de, por

---

de los datos relativos a la afiliación sindical de los trabajadores. Así se expone en la Sentencia del Tribunal Constitucional de 12 de diciembre de 2005 (RTC 2005\326); *"Entrando con ello en la queja referida a la supresión del complemento salarial, señala el Ministerio Fiscal que la relación entre la medida empresarial y la actividad sindical del demandante no ofrece lugar a dudas, pues así se reconoce expresamente, no siendo por ello necesario que el demandante aporte indicios de ninguna índole de que el comportamiento empresarial respondía a su actuación sindical. Lo controvertido se circunscribe, por tanto, a determinar si la supresión de este complemento de puesto de trabajo de indudable trascendencia económica vulneraba su derecho a la libertad sindical y, en particular, la garantía de indemnidad que veda cualquier diferencia de trato para el trabajador por el ejercicio de sus funciones sindicales, y concretamente el percibo de una menor retribución. Desde esa perspectiva, considera el Ministerio público que las Sentencias cuestionadas descartaron, mediante una argumentación en cierto sentido paradójica, la lesión del derecho a la libertad sindical del demandante, al señalar que el empleador había hecho valer una causa objetiva, ajena a todo móvil atentatorio a la libertad sindical, mediante la aportación de dos Sentencias precedentes que avalaban su tesis, para añadir seguidamente que el trabajador debía acudir a un nuevo proceso en reclamación de cantidad para discutir el impago del complemento de trabajo, proceso en el que se analizaría la procedencia o no del devengo en su aspecto de garantía de indemnidad retributiva".*

[915] GARCÍA NINET, J.I.: "Los derechos de los trabajadores a la protección de la seguridad y la salud en el trabajo y las obligaciones empresariales sobre estas mismas materias" en VV.AA; *Lecciones sobre la Ley de Prevención de Riesgos Laborales*, Servicio de Publicaciones Universitat Jaime I, 1997, pp. 111-113.

[916] Art. 23.1 d) y e) de la LPRL: "*El empresario deberá elaborar y conservar a disposición de la autoridad laboral la siguiente documentación relativa a las obligaciones establecidas en los artículos anteriores: d) Práctica de los controles del estado de salud de los trabajadores previstos en el artículo 22 de esta Ley y conclusiones obtenidas de los mismos en los términos recogidos en el último párrafo del apartado 4 del citado artículo. e)Relación de accidentes de trabajo y enfermedades profesionales que hayan causado al trabajador una incapacidad laboral superior a un día de trabajo. En estos casos el empresario realizará, además, la notificación a que se refiere el apartado 3 del presente artículo".*

[917] Art. 30.3 de la LPRL; "*Para la realización de la actividad de prevención, el empresario deberá facilitar a los trabajadores designados el acceso a la información y documentación a que se refieren los artículos 18 y 23 de la presente Ley".*

ejemplo, la relación de accidentes de trabajo, sin que conste en ellos el diagnóstico médico de los accidentados. Por tanto, para la cesión de las informaciones de referencia el empresario sólo precisará el consentimiento inequívoco del trabajador, el cual puede prescindirse si hay una normativa que lo habilite para tratar esa información, a tenor de lo citado en el del art. 11.2 a) de la LOPD y, en este supuesto podría darse ya que estas cesiones de datos están previstas en el citado art. 23.1 d) de la LPRL[918].

Ahora bien, según lo establecido en la LOPD[919], para ceder o comunicar datos que sí estén relacionados con la salud de los trabajadores y que sólo pueden ser tratados por el personal sanitario pertinente, será necesario el consentimiento expreso del trabajador. No obstante, dicho consentimiento no deberá ser solicitado si el empresario acredita una razón de interés general, o así lo dispone una Ley[920], y en la cesión de datos del profesional sanitario al INSS o a la entidad colaboradora[921] mediante el citado parte de baja la habilitación legal para realizar este trámite está prevista en el art. 2 del RD 575/1997[922], en el que se explica el procedimiento de notificación y

[918] Acerca de esta excepción vid., Informe Jurídico 434/2004 de la AEPD que establece: "*Como conclusión de lo hasta ahora expuesto, existirá una habilitación legal para la cesión de datos de los trabajadores afectados sin su consentimiento, sólo en el supuesto del cumplimiento de las obligaciones establecidas en el párrafo a) del apartado 1 del artículo 23 de la Ley 31/1995. En lo que se refiere a la cesión de los datos de salud de los trabajadores a los Delegados de Prevención, debemos señalar que, estos datos, dentro de los de carácter personal, tienen un régimen jurídico especial de protección. Ello tiene reflejo en el artículo 7. 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Persona, relativo a los datos especialmente protegidos, que indica: "Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente",* disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informesjuridicos /otras _cuestiones/common/pdfs/2004-0434_Tratamiento-conforme-a-la-legislaci-oo-n-de-prevenci-oo-n-de-riesgos-laborales.pdf [Consulta 07/07/2015].

[919] Art. 7.3 de la LOPD: "*Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente".*

[920] Lo establecido en el art. 7.3 de la LOPD coincide con lo requerido para cualquier cesión de datos sin consentimiento, sin que sea necesario que la información sea especialmente sensible.

[921]Véase Informe Jurídico 271/2009 de la AEPD, disponible en http://www.agpd.es/ portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2009-0271_ Cesi-oo-n-de-los-partes-de-baja-por-incapacidad-temporal-a-las-entidaes-gestoras-o-colaborado ras-de-la-Seguridad-Social.pdf [Consulta 24/06/2015].

[922] Art. 2.2. del RD 575/1997: *"En el plazo de tres días contados a partir del mismo día de la expedición del parte médico de baja, el trabajador entregará a la empresa la copia a ella destinada. La empresa cumplimentará los apartados correspondientes a ésta, conforme a lo establecido en los artículos 6 y 7 de la Orden del Ministerio de Trabajo y Seguridad Social, de 6*

comunicación de los partes de baja. Aun estando permitida la comunicación de datos médicos sin el consentimiento del titular es evidente que, en estos supuestos, esta cesión debe hacerse para atender las necesidades de control de los procesos de incapacidad laboral, ya que si se tuviera intención de utilizarse con otro objetivo se tendría que solicitar el consentimiento para cederlo a estas entidades –INSS o MCSS[923]-

Lógicamente, estas cesiones de datos médicos de los trabajadores conllevan la creación de un fichero público –INSS- , o de un fichero de naturaleza privada en el caso de las entidades colaboradoras de éste, los cuales tendrán los requisitos de creación ya citados anteriormente[924].

Dicho esto, también el art. 11. 2 f) de la LOPD[925]hace alusión a la cesión de datos relativos a la salud sin que sea preciso solicitar el consentimiento

---

de abril de 1983, por la que se dictan normas a efectos de control de la situación de incapacidad temporal en el sistema de la Seguridad Social, y remitirá la misma, debidamente sellada y firmada, a la Entidad Gestora en el plazo de cinco días contados a partir del mismo día de su recepción, utilizando a tal efecto cualquier medio autorizado que permita dejar constancia del hecho de la comunicación".

[923] Sobre el carácter confidencial de los datos médicos de los trabajadores y su posible requerimiento por las MATEPS vid., Sentencia del TSJ de Galicia de 2 de mayo de 2013 (RJCA 2013\603): *"Lo que se solicita en este caso fue la copia del informe médico de síntesis, en un expediente de determinación del contingencia, que no está previsto en esta disposición, además de que se refiere a datos médicos que estén en instituciones sanitarias, y aquí a quien se ha solicitado es al INSS, que no lo es, no presta servicios sanitarios, es una entidad que se encarga de la gestión y administración de las prestaciones económicas del sistema de SS, pues conforme a la redacción del artículo 57.1.a) del TRLGSS, en la redacción anterior al año 2011, en que fue derogado, por Ley 27/2011, de 1 de agosto de 2011 (RCL 2011, 1518, 1808) , se refería a la cesión por la Seguridad Social de los datos médicos para el reconocimiento y control de las prestaciones por riesgo durante el embarazo y lactancia, así como los que precise la inspección médica de los servicios públicos de salud para el ejercicio de sus competencias, en ninguno de cuyos casos nos encontramos. Por lo tanto, tiene que ser en un expediente por subsidio de incapacidad temporal, no como en este caso, que es expediente de determinación de contingencia, para fijar la misma, no para reconocer o mantener la prestación económica, y la tramitación y resolución de expedientes de declaración de contingencia, además, no la hace la Mutua, sino la Seguridad Social. No hay consentimiento del interesado. No hay habilitación legal. Y será cuando se ponga fin al procedimiento, que es competencia del INSS, cuando la Mutua podrá impugnar la resolución, y lo hará ante la jurisdicción social, donde podrá tener acceso a todos los documentos del expediente, conforme dispone el artículo 143 de la Ley 36/2011 (RCL 2011, 1845)" .*

[924] Vid., apartado 5.1.2 del presente Capítulo (ficheros públicos) y el apartado 4.2 del primer Capítulo.

[925] Art.11.2 f) de la LOPD: "*Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica".*

cuando ésta sea necesaria para solucionar una urgencia, para la cual se tenga que acceder al fichero de datos con esa información médica. Lo establecido en el citado artículo guarda relación con lo expresado en el art. 7.6 de la LOPD, que admite la citada excepción y la legitimidad del tratamiento sin conformidad del titular del dato, siempre que sea necesaria para proteger un interés vital del interesado. En el caso de los trabajadores, la excepción citada del consentimiento para la comunicación de datos sanitarios, operaría en aquellos supuestos en los que el empresario tuviera que cederlos para atender una urgencia que pudiera darse con ese trabajador en el propio centro de trabajo[926].

Cuestión diferente se plantea cuando las encargadas de la organización preventiva de la empresa son las MCSS[927], ya que estas son responsables del fichero y encargadas, por tanto, del tratamiento de datos de carácter personal, como así ha reconocido expresamente la AEPD[928]. Puede ocurrir que, estas MCSS pretendan incorporar esos datos en un registro informático propiedad de la empresa a la que pertenecen los trabajadores examinados, trasladando a esa base de datos toda la información médica que tengan sobre los empleados de ese centro de trabajo. Aunque a esa base de datos sólo tengan acceso el personal médico que realizó los controles, las autoridades sanitarias, y los empleados de la empresa encargados de su gestión y mantenimiento, es obvio que se está produciendo una cesión de datos a ese soporte informático propiedad de la empresa que contrata el servicio de prevención. Una cesión que excede de la habilitación del art. 22.4 de la LPRL, ya que el empresario

[926] DE MIGUEL, N.: *Tratamiento de datos personales en el ámbito sanitario. Intimidad versus interés público*, Tirant lo Blanch, Valencia, 2004, pp. 47-61; TASCÓN LÓPEZ, R.: *El tratamiento por la empresa de datos personales de los trabajadores. Análisis del estado de la cuestión.* Thomson- Civitas, 2005, pág.111; TRONCOSO REIGADA, A.: *La protección de datos…*op. cit., pp. 539-548.

[927] MUÑOZ RUIZ, A.B. Y MORENO SOLANA, A.: "La prevención de riesgos laborales y la protección de datos de carácter personal. El caso de la empresa "Air Spain"." Revista Información Laboral, núm. 4, 2014, pp. 3-6; GARCÍA GARNICA, M.C.: "La protección de los datos relativos a la salud de los trabajadores (a propósito de la STC 202/1999 de 8 de noviembre)", *Derecho Privado y Constitución*, núm.14, 2000, pp.129-164.

[928] Informe jurídico 189/2008 y 299/2009 de la AEPD; *"En consecuencia cuando la empresa contrate con una Mutua la protección de las contingencias profesionales de los trabajadores o la prestación económica de incapacidad temporal derivada de contingencias comunes, será considerada responsable del tratamiento de datos que realizan de acuerdo con las funciones que tiene legalmente atribuidas, y no con un mero tratamiento por cuanta de terceros. Podemos concluir que tanto las empresas encargadas de la Prevención de Riesgos Laborales como las Mutuas de Accidentes tienen la consideración de responsables del tratamiento de datos que realizan, al amparo de las funciones que tiene legalmente atribuidas".*

puede llegar a conocer más informaciones médicas de sus trabajadores de las que realmente le corresponden. En este punto, no se puede excluir la prestación del consentimiento expreso del trabajador para ceder esos datos, pues no se da ninguna de las situaciones descritas para que éste se pueda excepcionar[929].

[929] Vid., Informe Jurídico 411/2009 de la AEPD, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2009-0411_Servicio-prevenci-oo-n-riesgos-laborales-Cesi-oo-n-datos-salud-trabajadores-al-empresario.pdf[Consulta 25/06/2015].

CAPITULO IV: LAS TICS EN EL DESARROLLO DE LA RELACIÓN DE TRABAJO Y SU COLISIÓN CON EL DERECHO A LA PROTECCIÓN DE DATOS DE LOS TRABAJADORES.

1. CONDICIONES DE TRABAJO Y PRIVACIDAD DE LOS TRABAJADORES. 2. LAS TICS COMO MECANISMO DE ORGANIZACIÓN EN EL CENTRO DE TRABAJO. 2.1. Bases de datos de gestión de personal: la intranet. 2.2. La aplicación de mensajería instantánea whatsapp como medio de comunicación entre empresario y trabajador. 3***. EL USO DE LAS HERRAMIENTAS TECNOLÓGICAS COMO MEDIO DE CONTROL DE LOS TRABAJADORES Y SU COLISIÓN CON EL DERECHO A LA PROTECCIÓN DE DATOS.*** 3.1. Privacidad en el uso de los teléfonos de empresa. 3.2 Tratamiento de datos de trabajadores obtenidos por el control del ordenador de trabajo. 3*.2.1. Cuestiones generales. 3.2.2. Aplicación de los principios de la LOPD. 3*.3. Otros sistemas de control, supervisión y vigilancia y su posible afectación al derecho a la protección de datos. 3*.3.1. Los distintos sistemas de acceso al centro de trabajo.* 3*.3.2. Intromisión de los sistemas de videovigilancia en la protección de datos del trabajador. 3.3.3. Detectives privados como método para vigilar el cumplimiento de la prestación de trabajo. 3.3.4. El sistema de denuncias internas: "Whistlebowling".* ***4. EXTINCIÓN DEL CONTRATO DE TRABAJO Y DESTINO Y USO DE LOS DATOS DE CARÁCTER PERSONAL DE LOS TRABAJADORES.***

CAPITULO IV: LAS TICS EN EL DESARROLLO DE LA RELACIÓN DE TRABAJO Y SU COLISIÓN CON EL DERECHO A LA PROTECCIÓN DE DATOS DE LOS TRABAJADORES.

1. CONDICIONES DE TRABAJO Y PRIVACIDAD DE LOS TRABAJADORES.

Es obvio que la implantación de las TICS en el quehacer ordinario de la empresa ha modificado la forma de organizar el trabajo y de ejercer por parte del empresario las funciones de control sobre el trabajador, de acuerdo con las facultades que, en este sentido, le confiere el art. 20.3 del ET. Prueba de ello es el habitual recurso a los distintos medios tecnológicos e informáticos para el desempeño de la actividad laboral, siendo cada vez más numerosos los trabajadores que tienen acceso a la red para, por ejemplo, comunicarse con sus superiores y recibir las instrucciones de trabajo; para entablar relaciones comerciales o productivas con clientes de la empresa; para acceder a bases de datos con información acerca de su puesto de trabajo, sus condiciones y las tareas a desempeñar; o simplemente, para establecer contacto e intercambiar información con los demás trabajadores de la empresa[930].

Evidentemente, el manejo de estos medios tecnológicos está dirigido sobre todo aunque no sólo, a trabajadores que realicen tareas de dirección, coordinación, de gestión o administrativas en las que normalmente necesitan disponer de un equipo informático que le permita no sólo comunicarse con el empresario o con terceros sino también para configurar documentos y bases de datos con información relevante para la organización de la empresa[931]. Por otra parte, es igualmente frecuente que, dependiendo de la función que cada trabajador tenga en el centro de trabajo, se dote a los trabajadores de otras herramientas tecnológicas que permitan o faciliten su trabajo tales como una conexión a internet, un teléfono móvil, un correo corporativo, etc.

[930] ARIAS DOMÍNGUEZ, A. Y RUBIO SÁNCHEZ, F. *El derecho de los trabajadores a su intimidad,* Aranzadi, 2006, pp. 96-99.
[931] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos…,* op. cit., pp. 143-144.

El empresario, además, puede dar a través de medios informáticos instrucciones relativas al puesto de trabajo; que pueden ser de tipo general, de forma que vinculen a todos los trabajadores de la empresa, o específicas para cada trabajador o grupo de trabajadores que desempeñen una actividad determinada, instrucciones que aparecerán de forma precisa en el propio perfil de cada empleado. En estos supuestos, la plataforma puesta en marcha por la empresa constituye un medio de información para los trabajadores, por lo que es un mecanismo funcional a los efectos de establecer pautas de conexión entre el empresario y sus empleados, haciendo posible una información más rápida y directa.

Ahora bien, la implantación de estos sistemas en la empresa supone que muchos datos de los trabajadores del conjunto de la empresa y, en particular, de los que utilizan dichos medios informáticos queden grabados de manera automática en ficheros informáticos siendo en este momento en el que existe un tratamiento de información personal de los trabajadores. Porque no sólo se procesan datos destinados a la gestión de personal – productividad, nóminas, faltas de asistencia al trabajo, bajas laborales etc.-, sino que estos medios tecnológicos, establecidos para un mejor funcionamiento de la actividad laboral y con fines estrictamente productivos, pueden ser empleados por el empresario para supervisar a través de ellos la prestación de trabajo así como la forma de su desempeño, almacenando la información en el registro de las herramientas citadas – ordenador, teléfono de empresa, email corporativo, etc.-Esto es así en la medida en que, a diferencia de lo que ocurría con los mecanismos tradicionales, las TICS son capaces de registrar datos personales del trabajador gracias a los vestigios que deja en el sistema informático de la empresa[932].

Todo lo anterior obliga obviamente al empresario, en el ejercicio de estas competencias de dirección, ordenación y control, a cumplir con las exigencias de la normativa sobre protección de datos de carácter personal[933]. No

[932] VV.AA.: *Las relaciones laborales y la innovación tecnológica en España*, Fundación 1º de mayo, 2005, pp. 74, 77-83.
[933] Vid., apartado 4 del presente Capítulo.

obstante, existen algunas situaciones en las que el respeto al derecho a la protección de datos podría obviarse cuando se han establecido previamente pautas o códigos de uso de las herramientas tecnológicas puestas a disposición del trabajador[934], con la intención de impedir o limitar su uso para fines personales[935]. Sobre estas cuestiones versarán las páginas que siguen.

2. LAS TICS COMO INSTRUMENTO DE ORGANIZACIÓN DEL TRABAJO.

2.1. Bases de datos de gestión de personal: la intranet.

En las nuevas relaciones de trabajo es primordial la creación de una intranet en la que los empleados puedan consultar información relacionada con su puesto de trabajo como serían los objetivos de producción o los horarios de trabajo. De esta forma, en la intranet y en el perfil privado del trabajador pueden publicarse datos generales como los relativos a la productividad, insertando, por ejemplo, un listado en el que aparezcan todos los trabajadores de la empresa y el nivel de productividad obtenido en un determinado periodo

[934] CARDENAL CARRO, M.: "Desdramatizando el uso de internet en el trabajo" *Aranzadi Social*, núm.15, 2001, pág. 34; TOSCANI GIMÉNEZ, D. Y CALVO MORALES, D.*:* "El uso de internet y el correo electrónico en la empresa: límites y garantías", *Nueva Revista Española de Derecho del Trabajo*, núm. 165, 2014, pp. 197-224; SAN MARTÍN MAZZUCCONI, C.: "Navegar por internet en horas de trabajo... ¿Quién? ¿Yo?". *Revista Doctrinal Aranzadi Social*, núm. 19,2010, pp. 2-4; MONTOYA MELGAR, A.: "Nuevas tecnologías y buena fe contractual (Buenos y malos usos del ordenador en la empresa)" *Revista Relaciones Laborales*, núm.5-6, 2005, pp. 3-5.

[935] Sobre este aspecto el TS en su Sentencia de 6 de octubre de 2011(RJ 2011\7699) establece, ante la dispersión de criterios acerca de la permisibilidad o no del uso del equipo informático, un criterio único consistente en la desaparición de la expectativa de confidencialidad desde el mismo momento en el que el empresario le ha dado al trabajador instrucciones sobre cómo utilizar el ordenador de trabajo y, entre esas advertencias se encuentra la prohibición de su uso para fines que nada tengan que ver con el desarrollo de la prestación de trabajo .Este es el criterio mantenido también por las Sentencia del Tribunal Supremo de 26 de septiembre de 2007 (RJ 2007\7514) y 8 de marzo de 2011 (RJ 2011\932), ya que en las mismas se advierte que el uso moderado de los instrumentos tecnológicos de la empresa podría crear una expectativa de confidencialidad que debía ser respetada, pero no podía constituir un impedimento para controlar estos medios si previamente se había prohibido su uso y se había advertido el control. Sobre estas Sentencias vid., SAN CRISTÓBAL VILLANUEVA, J.M.: "El control laboral del uso del ordenador por parte del empresario: la consolidación del criterio doctrinal iniciado por el Tribunal Supremo. A propósito de la Sentencia del Tribunal Supremo de 8 de marzo de 2011", *Revista del Poder Judicial*, núm. 90, 2011, pp. 61-68; FERNÁNDEZ MÁRQUEZ, O.: "La utilización por los trabajadores de los bienes de la empresa: un enfoque desde el derecho de propiedad", *Revista española de Derecho del Trabajo*, núm. 148, 2010, pp. 891-894, 919-920;TASCÓN LÓPEZ, R.: "El lento (pero firme) proceso de decantación de los límites del poder de control empresarial en la era tecnológica", *Revista Doctrinal Aranzadi Social,* vol.5núm. 17, 2007, pp. 1995-2002; DE VICENTE PACHÉS, F.: "El control empresarial del ordenador. A propósito de la Sentencia del Tribunal Supremo -unificación de doctrina- de 26 de septiembre de 2007", *Tribuna Social* núm. 214, 2008, pp. 50-55;

de tiempo. Como pueden publicarse los horarios de trabajo de todos los trabajadores, permitiendo al trabajador conocer tanto el suyo como el de los demás compañeros de trabajo, aunque esto es más una medida que puede tener como fin proporcionar transparencia evitando que se produzcan situaciones discriminatorias en la empresa en lo relativo a la distribución de las horas de trabajo.

Por otro lado, la evolución tecnológica ha dado lugar a que la intranet se presente como un tablón en el que los sindicatos puedan colgar la información sindical para sus afiliados, si bien, como sucede con las órdenes de trabajo de carácter general no suelen, ni deben, contener ninguna información personalizada[936]; pero si la tienen, la simple publicación de ésta constituye un tratamiento que puede implicar el acceso a datos personales por parte de terceros[937]. Finalmente, en la intranet también pueden localizarse informaciones mucho más individualizadas relativas a aspectos de la propia contratación laboral del trabajador y del desarrollo de la misma tales como la nómina o los datos tributarios o de seguridad social.

---

[936] Sin embargo, la Sentencia de la Audiencia Nacional de 19 de diciembre de 2007 (JUR 2008\11648) establece la prevalencia del derecho a la libertad sindical sobre el derecho a la protección de datos, cuando esa información tiene como finalidad permitir que los afiliados conozcan una determinada noticia de interés sindical: *"Si bien es cierto que el derecho a la protección de los datos en el caso examinado impide que los datos personales del denunciante --nombre y apellidos-- se incluyan en una página de la Intranet corporativa sin que medie su consentimiento inequívoco, como señala el artículo 6.1 de la Ley Orgánica 15/1999 , sin estar amparado por alguna de las excepciones previstas en el apartado 2 del citado precepto. Sin embargo, esta cobertura de la acción sancionadora ha de quebrar cuando la nota informativa difundida por la Sección sindical del centro de trabajo, en este caso Caja Canarias, y en la que constan los datos del denunciante, tiene por finalidad la transmisión de noticias de interés sindical, permitir ese flujo de información entre el Sindicato y sus afiliados, entre los delegados sindicales y los trabajadores, de manera que se permita el ejercicio completo y cabal de la acción sindical, propiciando, como señalaba la doctrina constitucional trascrita en fundamentos anteriores, el desarrollo de la democracia y del pluralismo sindical, mediante este elemento esencial del derecho fundamental a la libertad sindical. El derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero. Este <<poder de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero >> (fundamento jurídico séptimo de la STC 292/2000, 30 de noviembre), ha de ceder cuando se enfrenta al ejercicio del derecho a la libertad sindical en los términos en que concurre en este caso, en el que se trata de proporcionar una información propia de la actividad sindical, no entendible sin el dato personal en cuestión, y limitada al ámbito del centro de trabajo".*

[937] AEPD: Guía de las relaciones…, op. cit., pág. 32-33.

De todo lo anterior se derivan una serie de informaciones de los trabajadores de carácter personal o profesional, pero individualizadas, cuyo tratamiento informático y su almacenamiento en el portal interno de la empresa ha de respetar los principios relativos a la protección de datos del trabajador.

Así, en primer lugar, el empresario debe tratar los datos de los trabajadores atendiendo a la finalidad concreta que no es otra que la funcionalidad necesaria en relación con la prestación laboral así como la de prestar un servicio de información a los trabajadores, inscribiéndola en el perfil personal de cada trabajador. Para ello el empresario tendrá que dar publicidad a esos datos de forma proporcional, sin utilizarlos para otros fines que no estén relacionados con el simple hecho de dar a los trabajadores una información más actualizada y directa de aquellos datos que pueden interesarle en un momento determinado de la relación laboral, ya sea en el desempeño de la misma o en relación con sus datos personales.

De este objetivo empresarial debe estar informado el trabajador, así como del tratamiento de sus datos, es decir, de la utilización de la intranet por parte del empresario como herramienta de comunicación y de la inclusión de la información que allí aparece en un fichero. Más aún cuando muchos de esos datos que el empresario publica en la intranet han sido facilitados previamente por el propio trabajador. Por lo que éste tiene que conocer que van a ser utilizados con esta finalidad y que pueden cederse a terceros, por ejemplo, a la entidad externa que se encargue de la creación de la web de la empresa y de configurar los contenidos si, además, es la competente para gestionar la aplicación e incluir la información de cada trabajador. El empresario tendrá, pues, que advertir al trabajador de la responsabilidad de esa base de datos a efectos de que éste pueda ejercitar los derechos que la LOPD le confiere como titular de esa información – acceso, rectificación, cancelación y oposición-.

Por otra parte, y si bien el consentimiento del trabajador para que el empresario pueda tratar datos dentro del ámbito laboral está exceptuado, esta regla no es absoluta ya que el mantenimiento de la relación contractual no le da

derecho al empresario a manejar libremente los datos del trabajador, o a realizar cualquier actuación en este sentido que constituya un tratamiento de datos sin que medie el consentimiento de éste. Por ejemplo, según criterio de la AEPD[938], la publicación de datos en la intranet sobre la productividad de los trabajadores requerirá el consentimiento de éstos, pues si bien el empresario está habilitado para ejercer un control sobre la producción sin que se solicite el consentimiento del trabajador, esto no lo faculta para que permiir que el resto de la plantilla conozca esa información; en la medida en que su publicación sin consentimiento no es necesaria para el mantenimiento de la relación contractual y, por tanto, éste no debe ser exceptuado. Lo mismo sucede con la cesión de datos, circunstancia de la que debe ser informado el trabajador requiriéndose su consentimiento para transmitir esos datos a otras empresas, como, por ejemplo, la misma encargada de la gestión de la intranet.

Finalmente, la utilización de la intranet de la empresa como canal de transmisión de información entre empresario y trabajador puede hacer que esa información de carácter personal de los trabajadores se pueda filtrar a un tercero, como por ejemplo otros trabajadores de la empresa. Razón por la que el empresario debe establecer las medidas de seguridad necesarias y en el nivel requerido (básico, medio o alto) para proteger la información privada de los trabajadores colgada en la intranet. Teniendo en cuenta, además, que alguna puede tener la categoría de dato especialmente protegido como, por ejemplo, la contenida en la nómina o la que pudiera reflejar algún dato relacionado con la discapacidad de ese trabajador necesaria para practicar alguna deducción o beneficio fiscal en su recibo salarial.

---

[938] Según la AEPD: "*El mencionado artículo legitima la implantación de las medidas que el empresario estime oportunas de vigilancia y control del trabajadores, pero es un control efectuado por el propio empresario al trabajador y la actuación descrita en la consulta lleva implícito un control efectuado al trabajador por sus propios compañeros, cuestión que parece distinta a la prevista en el mencionado artículo… En caso contrario, para amparar el tratamiento y cesión de datos debe obtenerse el consentimiento del trabajador, consentimiento que como hemos señalado al principio resulta difícil obtener en el ámbito laboral. Una solución para obtenerlo, sería incluir estas medidas en una cláusula del contrato de trabajo, para que el propio trabajador pueda conocer la política de las productividades antes de aceptar el puesto de trabajo*", vid., Informe jurídico 529/2009 de la AEPD, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/20090529_Comunicaciones-de-las-productividades-de-los-trabajadores-a-otros-trabajadores.pdf. [Consulta 21/07/2015].

2.2. La aplicación de mensajería instantánea whatsapp como medio de comunicación entre empresario y trabajador.

El uso de las aplicaciones que se pueden configurar en los teléfonos móviles de última generación también ha llegado al mundo de las relaciones laborales. De ahí que la cada vez más extendida utilización del programa de mensajería instantánea whatsapp[939] constituya en el centro de trabajo un medio más para realizar gestiones administrativas y propiciar la comunicación no sólo entre cliente y empresa[940], sino también entre empresario y trabajadores. Como consecuencia de la repercusión de este sistema en el ámbito laboral existen, hoy día, algunos Convenios Colectivos[941] que advierten acerca de cómo debe ser el uso de esta herramienta vinculada al móvil de empresa o, incluso, al teléfono personal del trabajador.

Obviamente, los datos intercambiados a través de la aplicación whatsapp deben ser protegidos de forma general conforme a la normativa sobre protección de datos ya que esa información constituye un dato de carácter personal, poniendo en relación este concepto con lo establecido en el Considerando 24 de la Directiva 2002/58/CE[942]que establece que toda la

[939] Según el estudio "Telco Trendsfor 2015+" realizado por Strategy, la consultora estratégica de PwC, este servicio "cuenta con más de 700 millones de usuarios en todo el mundo y por el cual se enviaron unos 30.000 millones de mensajes al día en 2014. España se encuentra a la cabeza en el uso de este tipo de mensajería, situándose como cuarto país del mundo con un 70% de penetración de este servicio entre los usuarios de telefonía móvil, por detrás de Sudáfrica (con un 78%), Singapur (72%) y Hong Kong (71%) y lejos de Italia (con 62%) o Reino Unido (34%)". Según datos oficiales de la empresa de mensajería, adquirida por Facebook en 2014, whatsapp había superado en septiembre de este año los 900 millones de usuarios activos. Fuente: http://www.strategyand.pwc.com/media/file/Telco-Trends-for-2015-eps.pdf. pág.11.

[940]Aunque el Dictamen núm. 24/2013 de la APDCAT, disponible en http://www.apdcat /media/dictamen/ca_568.pdf [Consulta 30/09/2015] deja clara la existencia de diversas vulneraciones a la LOPD en *WhatsApp,* sobre todo por deficiencias en cuanto al consentimiento y el deber de información del usuario, lo que supone un riesgo para la confidencialidad de las conversaciones que los abogados pudieran tener a través de la referida aplicación, por lo que es preferible que éstos utilicen otros medios de comunicación (por ejemplo, el correo electrónico con medios de protección criptográficos).

[941]Por ejemplo, en el Convenio Colectivo de Industrias Aderezo, Relleno, Envasado y Exportación de Aceituna de Sevilla (BOP Sevilla de 12 de junio de 2014) se incentiva el uso de whatsapp advirtiendo a los empleados que las llamadas al trabajo se podrán realizar a través de este mecanismo. Sin embargo, el Convenio Colectivo Provincial de Oficinas y Despachos de Zaragoza (BOP Zamora de 2 de mayo de 2014) prohíbe el uso de whatsapp dentro del centro de trabajo.

[942] Considerando 24 de la Directiva 2002/58/CE: *"Los equipos terminales de los usuarios de redes de comunicaciones electrónicas, así como toda información almacenada en dichos*

información registrada en los terminales informáticos forma parte de la esfera privada de los usuarios de las redes de telecomunicaciones. Evidentemente, el tratamiento de datos que se puede alcanzar a través de este medio se traduce en la grabación de las conversaciones de whatsapp en todos los terminales con los que se contacta, lo cual puede ser utilizado para un uso posterior distinto de la finalidad acordada entre empresario y trabajador como es la de ser un medio de comunicación entre ambos.

Parece lógico pensar que la finalidad del tratamiento de esos datos, almacenados a través del whatsapp, cuando se realiza a través de un dispositivo móvil proporcionado por el empresario al trabajador para la ejecución de sus funciones, no es otra que la transcripción de estas conversaciones como prueba[943] ante un supuesto incumplimiento de la prestación de trabajo[944]. A pesar de ser una práctica admitida en sede judicial[945], no parece del todo claro que este uso cumpla con el principio de

---

equipos, forman parte de la esfera privada de los usuarios que debe ser protegida de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Los denominados «programas espía» (spyware), web bugs, identificadores ocultos y otros dispositivos similares pueden introducirse en el terminal del usuario sin su conocimiento para acceder a información, archivar información oculta o rastrear las actividades del usuario, lo que puede suponer una grave intrusión en la intimidad de dichos usuarios. Sólo debe permitirse la utilización de tales dispositivos con fines legítimos y con el conocimiento de los usuarios afectados".

[943] Art. 90 de la Ley 36/2011: *"Las partes, previa justificación de la utilidad y pertinencia de las diligencias propuestas, podrán servirse de cuantos medios de prueba se encuentren regulados en la Ley para acreditar los hechos controvertidos o necesitados de prueba, incluidos los procedimientos de reproducción de la palabra, de la imagen y del sonido o de archivo y reproducción de datos, que deberán ser aportados por medio de soporte adecuado y poniendo a disposición del órgano jurisdiccional los medios necesarios para su reproducción y posterior constancia en autos".*

[944] *De forma general vid., BACARRIA MARTRUS, J.: "El caso whatsapp. Las aplicaciones de mensajería instantánea como medio de prueba en el procedimiento judicial",* Economist&Jurist, *Vol. 22, núm. 185, 2014, pp. 80-85.*

[945] Sentencia del TSJ de Cataluña de 15 de julio de 2014 (JUR 2014\243599): "*Por ello, añadía el Alto Tribunal, el derecho al secreto de las comunicaciones "no puede oponerse, sin quebrantar su sentido constitucional, frente a quien tomó parte en la comunicación misma así protegida...(por cuanto) la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados, el derecho posee eficacia erga omnes) ajenos a la comunicación misma...". O, y en otros términos, que "no hay "secreto" para aquel a quien la comunicación se dirige ni implica contravención de lo dispuesto en el artículo 18.3 de la Constitución la retención por cualquier medio del contenido del mensaje...dicha retención (la grabación en el presente caso) podrá ser, en muchos casos, el presupuesto fáctico para la comunicación a terceros, pero ni aun considerando el problema desde este punto de vista puede apreciarse la conducta del interlocutor como amparatoria del ilícito constitucional" de manera que "la grabación en sí -al margen de su empleo ulterior- sólo podría constituir un ilícito sobre la base del reconocimiento de un hipotético "derecho a la voz" que no cabe identificar en nuestro ordenamiento por más que sí pueda existir en algún derecho extranjero....(y dado) que*

calidad previsto en la LOPD, sobre todo si, como suele suceder, no se le informa previamente al trabajador del archivo de esas conversaciones ni de su posible uso para gestionar su comportamiento en la empresa que pueda ser detonante de un posible despido[946]. Por lo tanto, si existe procesamiento de la información, se trata de una circunstancia de la que debe ser informado el trabajador, siendo necesario su consentimiento para el tratamiento de datos, de conformidad con lo establecido en el art. 6.2 de la LOPD.

Si el trabajador conoce y ha sido informado del uso que ha de dar al móvil y sabe que por la propia naturaleza del sistema de mensajería las conversaciones mantenidas quedan grabadas, a menos que el propio trabajador las elimine, ello convierte en legítima la utilización de estos diálogos almacenados que podrían usarse para comprobar y atestiguar desde el uso correcto del sistema de comunicación hasta el l hecho de que los contactos se han realizado durante el tiempo de trabajo afectando al normal desarrollo de la prestación de trabajo[947], pasando por la forma en que ha de ser desarrollada la propia prestación laboral.

---

tal protección de la propia voz existe sólo en el Derecho español, como concreción del derecho a la intimidad y, por ello mismo, sólo en una medida en que la voz ajena sea utilizada ad extra y no meramente registrada, y aun en este caso cuando dicha utilización lo sea con determinada finalidad (artículo 7.6 de la citada Ley Orgánica 1/1982 (RCL 1982, 1197) : "utilización de la voz de una persona para fines publicitarios, comerciales o de naturaleza análoga")".

946 Sobre este asunto resulta interesante la Sentencia del TSJ de Madrid de 10 de junio de 2015 (JUR 2015\178247) en la que una trabajadora le comunica por whatsapp a su jefa de zona su intención de abandonar el trabajo. Es obvio que la utilización de la información grabada en el móvil, independientemente de la procedencia o no del despido, no es conforme al principio de calidad ni al de información ya que la trabajadora no fue advertida del uso que se le iba a dar a los datos, almacenados en el móvil de su jefa mediante la aplicación whatsapp, ni prestó su consentimiento para ello: "*Pues bien, en el supuesto de autos la actora solicita en primer lugar que se suprima en el Hecho Probado Quinto la frase que hace referencia a que por la tarde la encargada de zona se comunicó con la actora a través de la aplicación "whatsapp", reiterando ésta que no iba a volver al trabajo, y aduce la recurrente al efecto que dicho extremo no se encuentra amparado en prueba documental válida. Sin embargo, no es posible ignorar que la alegación de inexistencia de prueba válida no basta para sustentar la revisión del relato fáctico al amparo del artículo 193 b) de la LRJS , a lo que se ha de añadir que el intercambio de "whatsapp" entre la directora de zona y la demandante, en que ésta mantiene su posición de dejar el trabajo, ha quedado acreditado a través de la testifical, según se señala expresamente en el Fundamento de Derecho Segundo de la Sentencia, sin que dicha prueba resulte apta para la modificación del relato de hechos probados, por impedirlo la técnica suplicatoria".*

947 Sentencia del TSJ de Cantabria de 18 de junio de 2014 (PROV 2014, 180053): *"En el presente caso la conducta que se imputa al trabajador y que ha resultado debidamente probada es el uso de su teléfono móvil durante casi todo el trayecto que comprendía la ruta del día 1-8-2013. Resulta evidente que el uso continuado de un dispositivo móvil mientras se conduce un vehículo con pasajeros constituye un acto imprudente o negligente que además,*

Por otro lado, el empleado puede comunicarse mediante este método también con otros trabajadores de la empresa, los cuáles podrían notificar esas conversaciones al empresario, con una consecuencia negativa para el trabajador, independientemente de ser los encargados o no de realizar la gestión de personal y de certificar el cumplimiento de la prestación de trabajo. En estos casos se estaría produciendo una cesión de la información a terceros ajenos a la conversación mantenida, para la cual debería de haber mediado el consentimiento de ese trabajador. .

Por otra parte, el uso del whatsapp podría constituir una herramienta para controlar la efectividad del trabajador durante el tiempo de trabajo, ya que el empresario con la grabación del teléfono móvil de sus trabajadores en su terminal puede conocer cuántas veces ha consultado éste su whatsapp- fecha y hora de la última conexión- e incluso, guardar imágenes mostradas en su perfil, sin que el trabajador conozca esta actuación ni el uso que se le va a dar a esas informaciones filtradas por ese medio. En relación con esto hay que decir que, desde el momento en el que el empresario crea una base de datos con la información contenida en el medio de comunicación descrito y referida, por ejemplo, a la cantidad de veces que ese trabajador utiliza su whatsapp o a cualquier imagen grabada procedente de su perfil, se está produciendo sin duda un procesamiento de datos personales. Sin embargo, es muy posible que este tratamiento de datos no cumpla el objetivo inicial, relacionado con el establecimiento de este sistema como fuente de comunicación entre empresario y trabajador. Mucho menos si no ha sido admitido por parte de los empleados puesto que no se les ha advertido previamente de la existencia de un archivo con esa información ni tampoco han consentido esa utilización.

---

supone un evidente riesgo para la seguridad del servicio, lo que permite calificar tal actuación como falta laboral grave, tipificada en el apartado k) del Capítulo V del Laudo Arbitral de 24-11-2000. Estamos, no solo, ante una omisión de normas inexcusables o aconsejadas por la normal experiencia, lo que, sin duda, configura el concepto de imprudencia grave, sino también una actuación no ajustada a la diligencia exigible, según las circunstancias del caso concreto, de las personas, tiempo, lugar y sector de la realidad social en el que se actúa. Por tanto, de los hechos que obran en el relato fáctico, se desprende una negligencia especialmente grave en su actuar, que evidencia un quebrantamiento de los elementales deberes de fidelidad y buena fe que se aducen para su despido. Además, al constar la expresa prohibición empresarial de tales conductas, su comportamiento podría tipificarse también como transgresión de la buena fe contractual, indisciplina o desobediencia en el trabajo (apartado c) del Capítulo V)".

Información, pues, y consentimiento, son los requisitos necesarios para un uso y tratamiento empresarial de tal información que deberá fundarse en un objetivo igualmente publicitado, consentido y lícito.

3. EL USO DE LAS HERRAMIENTAS TECNOLÓGICAS COMO MEDIO DE CONTROL DE LOS TRABAJADORES Y SU COLISIÓN CON EL DERECHO A LA PROTECCIÓN DE DATOS.

Sin dejar de reconocer las ventajas que las TICS proporcionan a los procesos productivos, cabe reseñar el lado más oscuro de la utilización de estos medios en la empresa relacionado con el incremento de las facultades de control del empresario sobre el trabajador. Por un lado, esta supervisión más intensa del trabajador puede devenir del registro de las herramientas que el empresario ha cedido al trabajador para que efectúe su trabajo y, por otro, a través del control realizado mediante la instalación de mecanismos tecnológicos en el centro de trabajo[948]. El denominador común a estas dos formas de vigilancia de la prestación de trabajo es la afectación del derecho a la protección de datos de carácter personal de los trabajadores desde el mismo momento en que esa información personal, captada de una u otra manera, es tratada sin atender lo establecido en la LOPD[949].

Antes de analizar la posible colisión con el derecho a la protección de datos de los trabajadores, como se verá en los siguientes subapartados, es preciso hacer un breve análisis acerca de la implantación de estas medidas de supervisión, a efectos de comprobar su legalidad. Por este motivo y advertida la agresividad de la informática para la privacidad de los trabajadores se hace preciso acudir al análisis que realiza la doctrina constitucional sobre este asunto.

En todo caso, y como criterio general, debe acudirse a las Sentencias del Tribunal Constitucional 98/2000, de 10 de abril y 186/2000, de 10 de julio

[948] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos…,* op. cit., pp. 37-40.
[949] Vid., art. 3 c) de la LOPD.

[950]. De forma que el empresario tiene que cumplir a la hora de efectuar estas acciones de control a través de las TICS los siguientes requisitos: en primer lugar, se debe observar si el examen de esa herramienta tecnológica es susceptible de conseguir el objetivo propuesto; en segundo lugar, debe cuestionarse si existen otras formas menos restrictivas de los derechos fundamentales de los trabajadores o más moderadas que aseguren con igual eficacia el correcto desarrollo de la prestación del trabajo por el trabajador; y por último, habrá que valorar si de esa actuación empresarial se derivan más beneficios que perjuicios para el interés general[951].

3.1. Privacidad y control en el uso de los teléfonos de empresa.

La habilitación por parte del empresario de teléfonos móviles para los trabajadores de su empresa, además de una útil herramienta de trabajo, puede ser a la vez fuente de abundante de problemas jurídicos derivados del uso (adecuado o inadecuado, excesivo o impropio) que el trabajador hace de dicha herramienta con las repercusiones negativas sobre la productividad del trabajo, su dedicación, la difusión incorrecta de informaciones, o incluso sobre el excesivo gasto de la empresa derivado de una utilización desmesurada o inapropiada de los teléfonos. Pero también, y sobre todo y en lo que aquí interesa, problemas jurídicos derivados del control por parte del empresario,

[950] En este punto, tiene especial importancia la Sentencia 98/2000 del Tribunal Constitucional de 10 de abril (RTC 2000\98) que se pronuncia acerca de si la instalación de un sistema de audio complementario al mecanismo de grabación de imágenes, ya existente, es una medida idónea y necesaria para preservar la seguridad y buen funcionamiento de un casino, concluyendo que esta forma de vigilancia no se ajusta al principio de proporcionalidad que rige la modulación de los derechos fundamentales en general. Ese "plus de seguridad" que se pretende dar en el local de juego no justifica el sacrificio del derecho a la intimidad del trabajador que es escuchado a través de los micrófonos implantados en su puesto de trabajo, independientemente de que ese trabajador fuera conocedor de esa medida. Por lo que, en este supuesto, el empresario no se puede amparar en la facultad empresarial prevista en el art. 20.3 del ET para instalar este sistema de supervisión de los trabajadores. Sin embargo y en sentido contrario, la Sentencia 186/2000 del Tribunal Constitucional de 10 de julio (RTC 2000\186) considera que la medida de control consistente en la instalación de cámaras de videovigilancia en la zona de cajas, para supervisar el trabajo de un empleado concreto sobre el que existían sospechas acerca de sus conductas irregulares, si es acorde con el criterio de proporcionalidad y, por tanto, justificada e idónea para la finalidad pretendida por el empresario, que no es otra que verificar si el trabajador está realizando bien su prestación de trabajo.

[951] Sobre la aplicación del juicio de ponderación en la restricción de derechos fundamentales, vid., ARIAS DOMÍNGUEZ, A. Y RUBIO SÁNCHEZ, F.:*El derecho de los trabajadores a*…, op. cit., pp. 19-20; PARDO FALCÓN, J.: "El juicio de indispensabilidad: un avance de los derechos fundamentales en el ámbito laboral", *Temas Laborales*, núm. 39, 1996, pág. 60; DESDENTADO BONETE, A. Y MUÑOZ RUIZ, A.B.: *Control informático, video vigilancia y…,* op. cit., pp. 20-24.

también por medios informáticos vinculados a una base de datos, del uso que el trabajador hace del teléfono.

A este respecto, es claro que, para poder efectuar un cierto control del uso que el trabajador hace del teléfono de empresa, tan sólo es necesaria la simple visualización, incluso justamente por medios informáticos, de la factura telefónica que contiene el desglose de las llamadas realizadas por el trabajador. Por lo que el empresario puede conocer la cantidad de llamadas efectuadas con la mera consulta de este registro, averiguando si el empleado ha abusado del teléfono. Sin que sea necesario indagar más allá de ese listado de llamadas ni grabar o almacenar las conversaciones mantenidas en ese dispositivo, para poder determinar una conducta imprudente o negligente del trabajador[952].

En lo que aquí interesa, obviamente, el acceso y la mera consulta del recibo telefónico, no genera un tratamiento de datos de carácter personal. Sin embargo, el uso del teléfono de forma desmesurada puede crear en el empresario cierta desconfianza sobre un posible incumplimiento de la tarea encomendada y es, en ese momento, cuando puede establecer una supervisión del trabajo mucho más precisa a través del teléfono de empresa.

Por ello, estos registros de las conversaciones lesionan, si no se cumplen las exigencias legales, no sólo el derecho a la intimidad sino también el derecho a la protección de datos desde el mismo momento en que se crea un fichero con esas informaciones y no se cumple con lo establecido en la normativa sobre protección de datos. Se debe atender, en primer lugar, al

[952] Sentencia del TSJ de Cantabria (AS\1996\2748): *"Partiendo de la doctrina antes expuesta, concurren en la conducta del trabajador una serie de circunstancias a tener en cuenta, cuales son: a) tanto el tutor encargado del aprendizaje del actor como el Jefe de tráfico internacional de la empresa demandada que le hizo entrega del teléfono móvil, manifestaron que podía utilizar el teléfono para informar a su familia, lo que implica que no tuviese prohibido el uso para otros fines que los negociales; b) no existe ocultación ya que con la emisión de la factura se iba a saber o se podía conocer el origen de las llamadas; c) no ha existido requerimiento de pago a fin de que reintegrase el importe de las llamadas efectuadas con fines ajenos a la empresa, ni por tanto negativa al mismo; y d) el trabajador anticipó a la empresa el importe de gastos de viaje en cuantía de 133.005 ptas., cantidad superior a su salario mensual y a la factura telefónica. Estos datos revelan la falta de gravedad y culpabilidad en la conducta del trabajador, que en modo alguno puede calificarse como transgresión de la buena fe contractual en los términos legales".*

principio de calidad de los datos teniendo en cuenta que la finalidad de este procesamiento de información debe estar relacionada con la facultad que tiene el empresario de supervisión de la actividad laboral –art. 20.3 ET-. En este punto, se puede decir que se produce una vulneración del principio de calidad cuando esa recogida y tratamiento de la información no tiene como objetivo controlar al trabajador, ya que esto se puede realizar de una forma menos restrictiva para el derecho a la protección de datos de carácter personal, porque un registro de las llamadas que vaya más allá del acceso a la factura, es excesivo y poco o nada pertinente para la realización de la finalidad citada[953].

No obstante, podría admitirse esta práctica si el trabajador conociera la realización de esos controles y si hubiera sido informado del tratamiento de datos de las conversaciones mantenidas por medio del móvil de empresa y fuera la única forma de controlar la prestación de trabajo. En estos casos y según el criterio mantenido por el Tribunal Supremo[954], se rompe la expectativa de confidencialidad al haber advertido previamente el empresario la realización de estas acciones.

En respeto al principio de calidad el empresario también debe observar la debida proporcionalidad y pertinencia en relación con la medida adoptada , es decir, que el interés empresarial de conocer y tratar las conversaciones de los trabajadores, sostenidas a través de los teléfonos de empresa, sea primordial para cumplir con su tarea de control del trabajador, sin que pueda ser sustituido por otro método de supervisión de similar eficacia la prestación de trabajo. Por esta razón, y según el tipo de actividad que desempeñe el trabajador (como aquéllas en las que el teléfono sea el medio principal para la ejecución del trabajo encomendado, por ejemplo, el telemarketing), se admite jurisprudencialmente la posibilidad de control y registro de las llamadas con la

[953] SEMPERE NAVARRO, A.V.: "Sobre las nuevas tecnologías y las relaciones laborales" *Revista Aranzadi Social*, núm.15, 2002, pág. 8; GARCÍA NINET, J.I.: "Sobre el uso y el abuso del teléfono, del fax, del ordenador de la empresa en lugar y tiempo de trabajo. Datos para una reflexión en torno a las nuevas tecnologías" *Tribuna Social*, núm.127, 2001, pp.13-14.
[954]Sentencia del Tribunal Supremo de 6 de octubre de 2011, vid., nota 6.

finalidad exclusiva de fiscalizar la buena realización del servicio[955], siendo éste un examen vinculado al objetivo perseguido por el empresario[956].

Con carácter general, puede admitirse que, en los trabajos de telemarketing, si las conversaciones no pudieran ser intervenidas, esta prestación de trabajo no podría ser controlada ni dirigida, por lo que, dentro de la lógica de este tipo de prestación, esta supervisión es indispensable[957]. Pero siempre que el trabajador haya sido informado previamente de este hecho y se realice para comprobar la aptitud del trabajador respecto a la tarea encomendada. Si bien mediante este control que se hace sobre las llamadas recepcionadas es difícil que se averigüen datos que pertenezcan a la esfera privada del trabajador, teniendo en cuenta que el trabajo consiste en atender llamadas de clientes que acuden al servicio de telemarketing[958].

Centrando la atención en lo que aquí interesa, esto es en lo que al derecho a la protección de datos se refiere, ha de informarse necesariamente al trabajador si la utilización del teléfono de empresa tiene como consecuencia el almacenamiento de sus conversaciones en un fichero con el fin de tener los

---

[955] Sentencia del Tribunal Supremo de 5 de diciembre de 2003 (RJ 2004\313): *"Se trata de decidir, pues, si en este caso la medida empresarial denunciada como ilegal puede calificarse o no de proporcionada en relación con los dos derechos en juego: el del empresario a controlar la actividad de sus trabajadores y el derecho de éstos a no ser controlados en aspectos relacionados con el derecho a su intimidad, todo ello de conformidad con las pautas antes indicadas; o sea, teniendo en cuenta la doctrina constitucional sobre el derecho a la intimidad, pero sin olvidar que lo que aquí se resuelve es un problema de legalidad ordinaria, aunque este se halle conectado con el de constitucionalidad indicado…De todo ello en congruencia con lo ya indicado no se deduce que la empresa no pueda por esa vía atentar al derecho de intimidad de cualquier trabajador por cuanto, a pesar de todo, en esas conversaciones con los clientes pueden surgir comentarios que afecten a derechos fundamentales del trabajador incluidos dentro de la esfera de su intimidad en cuanto espacio excluido de cualquier posible intervención ajena –ideología política, afiliación sindical, libertad de expresión, etc.–, que, en cuanto fueran utilizados por el empleador podrían conducir a una declaración de nulidad en un proceso particular adecuado al caso. Pero lo que sí se deduce de todo ello es que el servicio de control que aquí se contempla no puede ser considerado contrario a los derechos invocados desde el punto de vista del derecho colectivo, puesto que la práctica empresarial se ha acreditado que va dirigida exclusivamente a controlar el trabajo de sus empleados con una finalidad meramente laboral y con medios ponderados y por lo tanto acomodados a las exigencias garantistas de la normativa denunciada como infringida".*

[956] Véase Sentencia del TSJ de Andalucía, de 4 septiembre de 2014 (AS 2014\3148).

[957] DESDENTADO BONETE, A. Y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y…*, op. cit., pp. 28-29.

[958] VV.AA: "Escuchas telefónicas a teleoperadoras", *Repertorio de jurisprudencia Aranzadi*, núm.4, 2004, pp. 3-8; RODRÍGUEZ LAINZ, J.L.: "SITEL y principio de proporcionalidad en la intervención de comunicaciones electrónicas" *Diario La Ley*, núm. 7689, 2011, pág. 1397-1400.

referentes necesarios para controlar la prestación laboral y su calidad. Si así fuera, el trabajador, partiendo del conocimiento de cuál es la finalidad empresarial en relación al tratamiento de datos, consentirá o no el tratamiento de su información personal. En este caso no se puede dar la excepción del consentimiento configurada en el art. 6.2 de la LOPD pues con estos hechos no se está procurando el mantenimiento de la relación laboral ni se puede justificar la ausencia de consentimiento para procesar la información basada en la facultad que tiene el empresario de controlar y supervisar la actividad del trabajador, ya que pueden existir otros medios orientados a cumplir esta función del empleador que no sean intrusivos de la esfera privada de los empleados.

En otro tipo de actividades que se desarrollan fuera del centro de trabajo el teléfono de empresa puede configurarse como un medio de control de los trabajadores, si en este dispositivo se instala un GPS con la intención de certificar la falta de actividad y supervisar los movimientos del trabajador. En este caso, hay que analizar si la medida implantada y el almacenamiento de datos obtenido a través del GPS se realizan conforme a derecho[959], teniendo en cuenta que la información captada por esta vía debe ser considerada dato de carácter personal.

Por este motivo y partiendo de la licitud de la medida de control,[960] es preciso ahora analizar si el empresario efectúa algún tipo de tratamiento de

[959] Informe Jurídico 0090/2009 de la AEPD, disponible en http://www.agpd.es/portalweb AGPD/canaldocumentacion/informesjuridicos/calidad/common/pdfs/2009-0090_Proporcionali dad-en-el-trata miento-de-datos-de-localizaci-oo-n.pdf [Consulta 28/09/2015].

[960] Acerca de la legalidad en la instalación de un GPS, en este caso en el vehículo de empresa, y del tratamiento de datos del trabajador en cuestión vid., la Sentencia del TSJ de Castilla la Mancha de 23 de marzo de 2015 (JUR 2015\95400);*"…es complemento indispensable del derecho fundamental del art. 18.4 CE "la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo". Por consiguiente, el Pleno del Tribunal ha señalado como elemento caracterizador de la definición constitucional del art. 18.4 CE, de su núcleo esencial, el derecho del afectado a ser informado de quién posee los datos personales y con qué fin. Ese derecho de información opera también cuando existe habilitación legal para recabar los datos sin necesidad de consentimiento, pues es patente que una cosa es la necesidad o no de autorización del afectado y otra, diferente, el deber de informarle sobre su poseedor y el propósito del tratamiento….En aplicación de esa doctrina, concluimos que no hay una habilitación legal expresa para esa omisión del derecho a la información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales, y que tampoco podría situarse su fundamento en el interés empresarial de controlar la actividad laboral a través de*

datos de los recogidos a través del GPS. Lógicamente, y siguiendo la ya conocida definición de tratamiento de datos dada por la LOPD[961], la captación de información por medio de la interceptación de un GPS en el teléfono de empresa supone sin duda un procesamiento de información personal que debe atender a los principios establecidos en la normativa sobre protección de datos

Es evidente que, si el empresario intenta conservar más datos de los recogidos del teléfono de empresa, de una u otra forma, de los estrictamente necesarios para controlar la prestación de trabajo, atenta contra el derecho a la protección de datos del trabajador. Y, desde luego, si ese registro de datos de las llamadas se realiza sin informar al trabajador previamente y sin haber obtenido su consentimiento.

3.2. Tratamiento de datos de trabajadores obtenidos mediante el control del ordenador de trabajo.

3.2.1. Cuestiones generales.

Los mayores problemas habidos respecto al tratamiento de datos de los trabajadores son aquellos relacionados con el registro y posterior almacenamiento de datos que puede hacer el empresario del ordenador del trabajador[962]. Una problemática que puede ser analizada teniendo en cuenta lo relativa a los archivos que mantenga el trabajador en el ordenador de empresa; la supervisión de la navegación por internet desde ese mismo equipo durante las horas de trabajo; y, por último, lo relacionado con el control del correo electrónico corporativo[963].

---

sistemas sorpresivos o no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia. Esa lógica fundada en la utilidad o conveniencia empresarial haría quebrar la efectividad del derecho fundamental, en su núcleo esencial. En efecto, se confundiría la legitimidad del fin (en este caso, la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos, art. 20.3 LET en relación con el art. 6.2 LOPD) con la constitucionalidad del acto (que exige ofrecer previamente la información necesaria, art. 5 LOPD), cuando lo cierto es que cabe proclamar la legitimidad de aquel propósito (incluso sin consentimiento del trabajador, art. 6.2 LOPD) pero, del mismo modo, declarar que lesiona el art. 18.4 CE la utilización para llevarlo a cabo de medios encubiertos que niegan al trabajador la información exigible".

[961] Vid., art. 3 c) de la LOPD.

[962] Como es lógico el empresario, al almacenar esa información en un fichero, debe cumplir las obligaciones y asumir las responsabilidades citadas en el apartado 4 del Capítulo tercero.

[963] CARDONA RUBERT, M.B.: "Tutela de la intimidad informática en el contrato de trabajo", *Revista de Derecho Social*, núm. 6, 1999, pp. 26-29; FERNÁNDEZ DOMÍNGUEZ, J.J. Y RODRÍGUEZ ESCANCIANO, S.: *Utilización y control de datos…*, op. cit., pp.102-103; DE VICENTE PACHÉS, F.: *El*

Hay que destacar, en primer lugar, que tanto la dirección de correo electrónico como la dirección IP[964] han sido incluidas por la AEPD en la noción de dato personal[965] por cuanto, con estos dos indicadores es posible identificar a una persona física, pudiendo el empresario, a través de este medio, reconocer a cada uno de los trabajadores.[966]. Se trata, por tanto, de datos personales, obtenidos a partir del registro del ordenador, en relación con los cuales el empresario debe atenerse, en cuanto a su almacenamiento y posterior tratamiento[967], a las exigencias derivadas de la normativa de protección de datos a la que se ha hecho múltiple referencia

Ante la falta de regulación específica sobre el tema el Dictamen 8/2001 sobre el tratamiento de datos en el contexto laboral del Grupo del art. 29, aprobado el 29 de mayo de 2002[968], hace un análisis de lo contenido en los arts. 8 y 10 del Convenio Europeo de Derechos Humanos[969] respecto a la

---

derecho del trabajador al…, op. cit., pp. 319-323; DE TISSOT, O.: "Internet et contrat de travail. Les incidences de la connexión á Internet sur les rapports employeur-salariés", *Droit Social*, núm. 2, 2000, págs. 150 y ss.

[964] La dirección IP sirve como un número de identificación que permite averiguar el nombre del trabajador al que previamente se le ha asignado esa dirección.

[965] Informe jurídico 0391/2007 disponible en http://www.agpd.es/portalwebAGPD /canaldocumentacion/informes_juridicos/transferencias_internacionales/common/pdfs/2007-0391_Cribrado-de-correo-electr-oo-nico.pdf [Consulta 28/07/2015].

[966] En este sentido se ha pronunciado la Sentencia de la Audiencia Nacional de 25 de mayo de 2006 (JUR\2006\174370): *"En consecuencia, la dirección del correo electrónico del denunciante causante de este procedimiento constituye dato de carácter personal en los términos definidos por el reiterado artículo 3.a) de la LOPD, en relación con el art. 4.1 del RD 1332/1994, y el uso del mismo mediante el acceso a las claves para su utilización por parte de un empleado de la empresa actora, (que trata en virtud de un contrato de prestación de servicios los datos personales de los clientes de una operadora telefónica), con el efecto de suplantación del titular y remitiendo mensajes a otros usuarios para fines particulares de dicho trabajador, constituye un claro caso de utilización incompatible, en el sentido de distinta, con la finalidad para la que el titular de esos datos de carácter personal se los cedió al responsable del fichero(AUNA) que luego encargo su tratamiento a otra persona, por lo que se produce una clara vulneración del principio de calidad de datos en los términos del artículo 4.2 de la LOPD, extremo éste, por lo demás, no discutido en ningún momento por la parte recurrente".*

[967] DESDENTADO BONETE, A. Y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y…,* op. cit., pp. 214-216.

[968] Fuente: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_es.pdf [Consulta 25/07/2015].

[969] Art. 8 del Convenio Europeo de Derechos Humanos: *"Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".* Art. 10 del Convenio Europeo de Derechos Humanos: *"Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar*

posible interceptación de las comunicaciones electrónicas por parte del empleador y la aplicación que hace en estas situaciones el Tribunal Europeo de Derechos Humanos de la Unión Europea[970]. En síntesis, se afirma que la jurisprudencia europea admite el posible uso personal, por parte del trabajador, de los dispositivos tecnológicos que la empresa haya puesto a su disposición, siempre que el empresario no le haya advertido previamente del carácter exclusivamente profesional de su utilización pues, sí se le han dado estas instrucciones, el empleado tendrá que limitar su uso a lo establecido en las mismas.

La Recomendación CM/Rec (2015) Comité de Ministros del Consejo de Europa sobre el tratamiento de datos personales en el contexto de empleo, de 1 de abril de 2015, ha establecido algunas instrucciones acerca de cómo tendrán que ejecutarse las comunicaciones electrónicas en el centro de trabajo para no afectar a la privacidad de los trabajadores[971]. Estas exigencias giran en

---

informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa. 2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, 12 13 condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial".

[970] En el mismo sentido, Sentencia del TEDH 3 abril 2007 (Caso Copland contra Reino Unido) (TEDH 2007\23) y Sentencia del TEDH 16 de febrero de 2000. (Caso Aman contra Suiza) (TEDH 2000\87). Recientemente la Sentencia del TEDH de 12 de enero de 2016 (Caso Barbulescu vs Rumania)(JUR\2016\11790), ha admitido el acceso al correo electrónico del trabajador por parte del empresario si anteriormente se ha advertido esa supervisión. Aunque en el pronunciamiento judicial existe un interesante voto particular en el que se establece que el trabajador tendrá que tener un conocimiento exacto de las limitaciones y restricciones al uso de los medios tecnológicos para usos no profesionales y concluye que si no se produce esa información esta actuación de registro del email es restrictiva de derechos como los recogidos en el art. 8 del CEDH.

[971] Art. 14 de la Recomendación CM/Rec (2015): "*1.Los empleadores deben evitar interferencias injustificables e irrazonables con el derecho de los empleados a la vida privada. Este principio se extiende a todos los dispositivos técnicos y las TIC utilizadas por un empleado. Las personas interesadas deben estar debidamente informados y de forma periódica, en aplicación de una política de privacidad clara, de conformidad con el principio 10 de la presente recomendación. La información proporcionada debe mantenerse al día y debe incluir el propósito del tratamiento, la preservación o el período de copia de seguridad de los datos de tráfico y el archivo de las comunicaciones electrónicas profesionales..2. En particular, en el caso de tratamiento de datos personales relativos a páginas visitadas por el empleado en Internet o Intranet, se debe dar preferencia a la adopción de medidas preventivas, como el uso de filtros que impiden que determinadas operaciones, y para la clasificación de las posibles monitoreo de los datos personales, dando preferencia por controles aleatorios no individuales*

torno al mantenimiento de la privacidad del trabajador en aquellas situaciones en las que el empresario quiere realizar un tratamiento de su información personal obtenida por el control del ordenador de trabajo. En parecido sentido se ha manifestado la OIT[972] al establecer que, cuando los trabajadores sean objeto de medidas de vigilancia, deberían ser informados de antemano de las razones que justifican el control; de las horas en las que tiene lugar; de los métodos y técnicas utilizados; y de los datos que serán almacenados, tratando el empleador de reducir al mínimo su injerencia en la vida privada de los trabajadores.

3.2.2. Aplicación de los principios de la LOPD.

A partir de lo dicho, y para que el tratamiento de los datos del que se está hablando pueda ser legítimo, es necesario atenerse a una serie de requisitos:

En primer lugar, ese tratamiento de información debe responder al *principio de calidad*, es decir, los datos registrados tienen que ser tratados de forma adecuada, pertinente y no excesiva; para una concreta finalidad que, en este caso, es la relacionada con la comprobación por parte del empleador de la correcta utilización del ordenador para el cumplimiento de la prestación de

sobre los datos que sean anónimas o de alguna manera agregados..3. El acceso de los empleadores a las comunicaciones electrónicas profesionales de sus empleados que estén informados con antelación de la existencia de esa posibilidad sólo puede ocurrir, cuando sea necesario, para la seguridad u otras razones legítimas. En el caso de los empleados ausentes, los empleadores deben tomar las medidas necesarias y prever los procedimientos adecuados destinados a facilitar el acceso a las comunicaciones electrónicas profesionales sólo cuando dicho acceso es por necesidad profesional. El acceso debe realizarse de la manera menos intrusiva posible y sólo después de haber informado a los trabajadores afectados. .4. El contenido, el envío y recepción de las comunicaciones electrónicas privadas en el trabajo no debe ser monitoreado bajo ninguna circunstancia. .5. A la salida de un empleado de una organización, el empleador debería adoptar las medidas organizativas y técnicas necesarias para desactivar automáticamente la cuenta de mensajería electrónica del empleado. Si los empleadores necesitan recuperar el contenido de la cuenta de un empleado para la buena marcha de la organización, deben hacerlo antes de su salida y, cuando sea posible, en su presencia".

[972] OIT: Repertorio de recomendaciones prácticas sobre la protección de los datos personales de los trabajadores, Ginebra, octubre, 1997, disponible en http://www.ilo.org/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/normativeinstrument/wcms_112625.pdf [Consulta 25/07/2015]

servicio encomendada[973]. En este sentido, y para no atentar contra el derecho a la protección de datos y cumplir de alguna forma con el objetivo de control, que es realmente lo que debe realizar el empresario, puede sostenerse que sólo debería acumularse la información absolutamente necesaria[974], por ejemplo, el número de visitas a internet y el tiempo que ha empleado el trabajador en las mismas, sin que sea necesario ni correcto registrar el contenido íntegro de esas visitas[975]. Se podría admitir su registro si el empresario hubiera advertido previamente al trabajador el sentido y finalidad de esa actuación, así como el archivo de la información captada por esa vía.

Estos controles deben realizarse a un trabajador concreto o de forma masiva, pero normalmente se harán sobre aquellos trabajadores de los que el empresario tenga alguna sospecha acerca del uso desmesurado del ordenador de trabajo. La duración de este registro será limitada, es decir, durante el tiempo necesario para poder cerciorarse, el empresario, del posible incumplimiento de la prestación de trabajo. De esta forma, la información tratada, aunque limitada, sería suficiente para la labor de control del trabajo del trabajador y del cumplimiento de sus obligaciones, sin necesidad de obtener y tratar otras informaciones cuyo procesamiento, por ser no imprescindibles para el fin de control, pueden colisionar con el derecho a la protección de datos[976].

Por otra parte, el email corporativo también puede servir como canal de comunicación entre empresario y trabajador; para notificarle a éste, por

[973] GONZÁLEZ ORTEGA, S.: "La informática en el seno de la empresa poderes del empresario y condiciones de trabajo" en VV.AA: *Nuevas tecnologías de la información y la comunicación y Derecho del trabajo*, Bomarzo, 2004, pág. 48.
[974] Según COLÁS NEILA, E. el registro de los contenidos de los correos corporativos por el empresario, tan sólo debe hacerse si del análisis de los envíos realizados por el trabajador se puede deducir un uso ilícito o abusivo del email pudiendo, entonces, acceder a los mensajes si la simple visualización del resto de datos no es prueba suficiente de la fraudulenta utilización del correo electrónico por parte del trabajador, en *Derechos fundamentales del trabajador en la era digital: una propuesta…,* op. cit., pp. 216-217.
[975] Sobre la vigilancia del trabajador a través del ordenador de trabajo vid., THIBAULT ARANDA, J.: *Control multimedia de la actividad laboral*, Tirant lo Blanch, 2006, pp. 108-110; MARIN ALONSO, I.: *El poder de control empresarial sobre el uso del correo electrónico en la empresa. Su limitación en base al secreto de las comunicaciones*, Tirant lo Blanch, 2005, pp. 168-169; SUÁREZ DE SÁNCHEZ, A.: "El acceso por el empresario al correo electrónico de los trabajadores", *La Ley*, núm. 1417, 2002, pp. 7-12.
[976] DESDENTADO BONETE, A. Y MUÑOZ RUIZ, A.B.:*Control informático, videovigilancia y…*, op. cit., pp. 97-104.

ejemplo, su horario laboral, el recibo salarial o datos relativos a su salud laboral, produciéndose en estos casos el envío de información confidencial del trabajador[977]. Esta información puede estar relacionada, incluso, con la notificación al trabajador, por parte de los servicios de prevención, de los resultados de los reconocimientos médicos, los cuáles valoran su aptitud para desempeñar una determinada tarea en la empresa. A este respecto, y como se ha dicho, el empresario sólo puede conocer, archivar y tratar aquella información que tan sólo revele la calificación profesional del trabajador. Por lo que, si lo que pretende averiguar y procesar información obtenida del mail del trabajador que revele detalles o circunstancias más personales e íntimas referidas, por ejemplo, a su salud, está obligado a respetar lo establecido en la normativa sobre protección de datos[978].

Respecto del *principio de información*, obviamente, si no se le ha informado previamente a los trabajadores del registro del ordenador, éstos tampoco conocerán si con esos datos se va a crear un fichero de datos y quién va a ser su responsable. A mi juicio, esta información tiene que darse porque, lógicamente, en el ejercicio del control del ordenador, accediendo al contenido de lo archivado y de las navegaciones hechas por internet, siempre se va a producir un tratamiento de información personal, incluyendo a veces información especialmente protegida –salud, ideología, etc.--. Sobre todo teniendo en cuenta la naturaleza informática del medio que se va a supervisar y lo difícil que resulta separar el contenido de los registros realizados en el ordenador; a menos que se prevea la instalación de un software que tan sólo establezca la cantidad de tiempo invertido en utilizar el equipo informático para fines personales.

[977] Sobre el acceso al ordenador de empresa ejercido por el empresario cuando éste ha prohibido que el trabajador pueda utilizarlo para fines personales, resulta interesante el voto particular esgrimido en la Sentencia del Tribunal Constitucional 241/2012 de 17 de diciembre , el cual aboga por el respeto al derecho fundamental a la protección de datos del trabajador aunque éste no haya respetado las instrucciones empresariales dadas de forma previa al inicio de la relación laboral o, mejor dicho, al comienzo del manejo del ordenador de empresa.
[978] Vid., apartado 3.2 del Capítulo III.

Dada la relevancia que tiene la prestación del *consentimiento* del titular del dato para poder tratarlo[979], en estos supuestos de vigilancia del equipo informático se puede decir que, atendiendo a lo establecido en el art. 6.2 de la LOPD en conexión con el art. 20.3 del ET, éste podría ser exceptuado[980], teniendo en cuenta, por un lado, la habilitación legal existente para que el empresario establezca las *medidas más oportunas de vigilancia y control* de la prestación de trabajo; y, por otro, la necesidad de tratar esos datos obtenidos por el control del ordenador para el mantenimiento (que es como decir gestión) de la relación laboral. De forma que el empresario estará legitimado para tratar datos, obtenidos en el cribado del email o del ordenador de empresa, sin consentimiento pero siempre que la cuenta de correo sea la que ha proporcionado para desarrollar la actividad laboral y se informe al trabajador previamente sobre ese filtrado de datos y su archivo[981]. En consecuencia, en los supuestos en que el procesamiento de la información personal puede hacerse por el empresario sin el consentimiento de los trabajadores, el derecho a ser informados se convierte en primordial.

En este mismo sentido, la AEPD[982] ha aceptado igualmente la facultad empresarial de acceder al contenido del ordenador del trabajador, en cuanto instrumento de trabajo proporcionado para esta tarea, así como tratar la información captada[983], siempre que se cumpla con el requisito de información previa que abarca tanto la existencia del tratamiento de datos como la finalidad y calidad del mismo.

Fuera de estos supuestos, el tratamiento de datos sólo será posible previo el consentimiento del trabajador. En todo caso, habrá que analizar qué

[979] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos…,* op. cit., pp.166-169.
[980] Art. 20.3 del ET; *"El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso".*
[981] Vid., Informe jurídico 247/2008 de la AEPD, disponible en
[982] Informe jurídico 391/2007 de la AEPD.
[983] En sentido contrario a esta apreciación de la AEPD, vid., GOÑI SEÍN, J.L: "Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos", *Justicia Laboral*, núm. 39, 2009, pág. 31.

datos son los que quiere procesar el empresario pues el tratamiento de los constitutivos de un simple control del número de emails enviados o de la cantidad de vistas a las distintas páginas webs de internet, manteniendo la opacidad de estas actuaciones del trabajador, se podría hacer sin que mediara el consentimiento. Como tampoco es obviamente exigible cuando haya una autorización judicial que valide estas conductas empresariales, lo que, además, sirve para validarlas como medio de prueba en el proceso judicial[984].

3.3. Otros sistemas de control, supervisión y vigilancia y su posible afectación al derecho a la protección de datos.

La llegada de las nuevas tecnologías a la empresa ha agilizado trámites relacionados con la actividad empresarial, pero también ha hecho que el empresario pueda establecer sistemas más sofisticados de control de los trabajadores para supervisar el efectivo cumplimiento de su jornada laboral o el desarrollo de la prestación de trabajo para la que ha sido contratado. El uso de estos mecanismos con esta finalidad puede llegar a convertir al trabajador en una persona demasiado vulnerable pues propician que se puedan supervisar casi todos los movimientos realizados dentro de la empresa en su tiempo efectivo de trabajo. Así pues, se hace preciso analizar esas prácticas desde el punto de vista de la protección de datos del trabajador, para sopesar si se cumple el necesario equilibrio entre el poder empresarial y el ejercicio de este derecho del trabajador, teniendo en cuenta que, muchas de las informaciones captadas y almacenadas como consecuencia de la vigilancia de la prestación de trabajo, deben ser consideradas datos de carácter personal.

Quedan así afectados sistemas de control en el acceso y salida del centro de trabajo o de presencia o de abandono del puesto. E igualmente pueden ser catalogada como información personal de los trabajadores las imágenes captadas por las cámaras de video vigilancia instaladas en la

[984] DEL REY GUANTER, S.: "Nuevas técnicas probatorias, obtención ilícita de la prueba y derechos fundamentales en el proceso laboral", *Revista Española de Derecho del Trabajo,* núm. 37, 1989, pág. 63-76; BAYLOS GRAU, A.: "Medios de prueba y derechos fundamentales. Especial referencia a la tutela de estos derechos" en AGUSTÍ JULIÁ, J.: *La prueba en el proceso laboral*, Cuadernos de derecho judicial, 1998, pág. 15 y ss.

empresa e, incluso, los archivos de voz[985] que pudieran grabarse por la utilización de aplicaciones informáticas instaladas en los teléfonos móviles puestos a disposición de los trabajadores, los cuales identifican a un trabajador concreto como consecuencia de la vinculación existente de ese trabajador con ese terminal. Como también pueden estarlo, en cuanto que recurren a los métodos informáticos, formas de realizar denuncias acerca de comportamientos irregulares de los trabajadores en la propia empresa, gracias a la instalación de un buzón online e interno cuya función principal es almacenar información acerca de las actuaciones negligentes de los empleados puestas de manifiesto por otros trabajadores o terceros. Algo muy habitual, por ejemplo, en las empresas de servicios. Ciertamente, cuando se produce el control del trabajador a través de medios ligados a las TICS es lógico que se produzcan grabaciones de datos como consecuencia, sobre todo, de la configuración de estos sistemas informáticos que llegan a tratar información personal de forma casi simultánea a la realización de la supervisión del trabajador.

Otra de las formas de control relacionadas con la certificación del cumplimiento de la prestación de trabajo, que puede afectar al derecho a la protección de datos, es la contratación de detectives privados. Se trata ciertamente de una forma de control todo menos que novedosa pero relevante aquí en la medida en que esos profesionales obtienen información que puede tener la naturaleza de datos (fotografías, imágenes, vídeos, grabaciones, etc.) de carácter personal y que luego son tratados (además de la propia información elaborada por el detective) en el marco de ficheros informáticos para, a su vez, ser comunicados al empresario y, posteriormente, procesados por éste[986].

[985] El art. 5.1 f) del RDLOPD considera dato de carácter personal a *"cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo susceptible de recogida, registro, tratamiento o transmisión concerniente a personas físicas identificadas o identificables".*
[986] Véase apartado 4.3.3 del presente Capítulo.

3.3.1. Los distintos sistemas de acceso al centro de trabajo y su posible colisión con el derecho a la protección de datos de carácter personal.

Antes de la implantación de las TICS en la empresa era posible manejar un sistema de horarios y asistencia tan sólo con emplear unas cuantas hojas de papel. Dichos días son historia y no sólo por el hecho de que pueden ser defectuosos al no ser tan precisos como los electrónicos y poder generar confusión a la hora de contabilizar las horas trabajadas. Actualmente existen sistemas sofisticados que incorporan estrategias y dispositivos para la captura de datos de forma rápida, organizada y segura.

Los sistemas de control de acceso al centro de trabajo que utilizaban reportes de papel implicaban un enorme gasto de tiempo y dinero al necesitar empleados que se dedicaran en exclusiva a estas funciones de control de los reportes de entrada y salida del centro de trabajo, así como la elaboración de forma manual de los cuadrantes con la asistencia mensual o diaria de cada trabajador al centro de trabajo. Además, dichos reportes podían ser poco fiables debido a la posible manipulación de la información con la finalidad de, por ejemplo, consignar más horas de trabajo u ocultar retrasos en la llegada al centro de trabajo; así como por la práctica, a veces de difícil control, de la firma por otro trabajador, simulando su presencia o ausencia del centro de trabajo

En cambio, los sistemas modernos para el control laboral basados en técnicas informáticas no sólo son mucho más precisos sino que también tienen la capacidad de mostrar, de forma detallada, todas las características de los momentos de presencia y de ausencia del trabajador en la empresa en relación con su jornada de trabajo permitiendo acceder a esta información de manera más rápida y organizada. Motivo por el que las empresas han instalado de forma muy generalizada sistemas como , el control de acceso mediante una tarjeta magnética o con una clave facilitada por la empresa; los controles biométricos[987]; las etiquetas de identificación; y los sistemas RFID o de radiofrecuencia.

[987] Sobre los sistemas de control biométricos, características y tipología vid., AREITIO BERTOLÍN, J. Y AREITIO BERTOLÍN, T.: "Análisis en torno a la tecnología biométrica para los sistemas

Lógicamente, estos sistemas favorecen el registro de la información personal[988] recogida a través de ellos, por lo que este archivo, en sí mismo, constituye un tratamiento de datos a los que le es de aplicación lo contemplado en la LOPD[989]. A esta caracterización general hay que añadir el riesgo de que la recopilación de estos datos permita obtener y tratar, a partir de la primera captación que se hace de ellos, otros datos accesorios no necesarios para la identificación del control de acceso de ese trabajador concreto. Pudiendo revelarse, por ejemplo con la utilización de mecanismos basados en la biometría[990], datos relativos a la salud del trabajador[991] calificados como especialmente protegidos por la LOPD[992]. Por estos motivos, los mecanismos menos intrusivos del derecho a la protección de datos de carácter personal son los sistemas de proximidad (fichaje a través de tarjeta magnética o introduciendo una clave personal de acceso) y los sistemas basados en la radiofrecuencia los cuales permiten la lectura/escritura de datos a distancia, insertos en tarjetas a través de mecanismos de radiofrecuencia.

---

electrónicos de identificación y autenticación" *Revista Española de electrónica*, núm. 630, 2007, pp. 52-58.

[988] Respecto de la catalogación como datos de carácter personal de las informaciones captadas en los sistemas de control de acceso, vid., Sentencia del TJUE de 30 de mayo de 2014 (asunto C-342/12, Worten), disponible en http://curia.europa.eu/juris/document: *"Dado que los datos que figuran en un registro del tiempo de trabajo se refieren a los períodos de trabajo diario y a los períodos de descanso de cada trabajador, el Tribunal concluye que son datos personales en el sentido del artículo 2, letra a), antes citado, puesto que se trata de "información sobre una persona física identificada o identificable".*

[989] Sobre la aplicación de controles basados en la biometría y su confrontación con el derecho a la protección de datos, véase el art. 18 de la Recomendación CM/Rec (2015): *"18.1. La recogida y posterior tratamiento de los datos biométricos sólo deben llevarse a cabo cuando sea necesario para proteger los intereses legítimos de los empleadores, empleados o terceros, sólo si no existen otros medios menos intrusivos disponibles y sólo si van acompañados de las salvaguardias apropiadas, incluido las adicionales salvaguardias previstas en el principio 21. 18.2. El tratamiento de datos biométricos debe basarse en métodos científicamente reconocidos y debe estar sujeto a los requisitos de seguridad estricta y proporcionalidad".*

[990] Vid., Informe jurídico 0324/2009 de la AEPD, disponible http://www.agpd.es/portalwebAGPD /canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2009-0324_Acceso-al-dato-huella-d-aa-ctilar-de-empleados-de-una-empresa-por-otra.-Encargado-del-tratamiento.pdf [Consulta 22/07/2015].

[991] Ejemplo de ello, son los relojes biométricos de huellas digitales, patrón del iris, estructura de su voz o forma y aspecto de su escritura manuscrita.

[992] Art. 7.3 LOPD: *"Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente".* Este aspecto queda determinado de forma más precisa en el RGPD, puesto que establece dentro de las definiciones el concepto de dato biométrico (art. 4.14), aspecto que no estaba previsto en la Directiva 95/46/CE.

El empresario, respecto de los datos almacenados, tendrá que establecer cuál es la finalidad perseguida con la recopilación de estos datos de los trabajadores, y si ésta es determinada, explícita y legítima de acuerdo con lo establecido en el art. 4 de la LOPD que regula el reiteradamente mencionado *principio de calidad* de los datos. En un principio, el tratamiento de datos realizado por parte del empresario tiene que tener como finalidad únicamente controlar el acceso de los trabajadores a la empresa así como el cumplimiento de la jornada de trabajo en virtud de la habilitación legal otorgada por el art. 20.3 del ET. Si es así, el uso del dato puede, y debe, ser proporcionada y no excesiva respecto de la satisfacción de los intereses empresariales y del derecho del trabajador a la protección de datos[993].

Haciendo referencia a la captación de datos a través de los denominados sistemas biométricos[994] el Tribunal Supremo, en su Sentencia de 2 de julio de 2007 (recurso 5017/20013)[995], establece que la instalación de

[993] Sentencia del Tribunal Superior de Justicia de Murcia de 25 de enero de 2010 (AS 165/2010): "*…pues no existe constancia de la utilización de tales datos para fines diversos y porque con ocasión de la lectura de la huella digital no se puede ver la imagen de la huella ni puede ser captada por terceros, quedando todos los datos del sistema guardados en los ordenadores de la empresa a efectos de su custodia, según refleja el apartado decimosegundo de los hechos declarados probados; y ello porque, aunque la huella digital tenga la consideración de un dato personal , no existe la prohibición absoluta respecto de su recogida y tratamiento, sino que, por el contrario, de conformidad con los términos del artículo 4 de la LO15/1999, cabe tal recogida y tratamiento "cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido". Estima esta sala que el control de acceso a las instalaciones de la empresa constituye una finalidad legitima, concreta y que fue suficientemente puesta de manifiesto a los trabajadores y que tal medida de control, que vincula la lectura de las huellas digitales a los datos de identidad de los trabajadores existentes en la empresa, es adecuada, pertinente y no excesiva"*.

[994] Documento de trabajo sobre biometría del Grupo Trabajo del art. 29 en el que se expone que: "*Un dato biométrico tiene que ser: universal, resultante de la captación de la muestra de un rasgo físico o biológico de todo ser humano; único, distintivo y peculiar de esa persona a la que se pretende identificar; y permanente, que significa la perpetuidad de esos rasgos físicos o biológicos*", disponible en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_es.pdf [Consulta 04/05/2015].

[995] RJ 2007\6598. Véase en el mismo sentido: Sentencia del TSJ de Canarias de 21 de julio de 2009 (JUR 2009\446907): *"Es cierto que el Gobierno de Cantabria se esfuerza en subrayar que el algoritmo informatizado no sirve por sí mismo como elemento de identificación de personas. Desde esa perspectiva, es como si pretendiera negar que se tratase de un dato de carácter personal. No obstante, de acuerdo con el artículo 3 a) de la Ley Orgánica 15/1999, por dato de carácter personal ha de entenderse "cualquier información concerniente a personas físicas identificadas o identificables". Por tanto, en la medida en que el registro en cuestión se integra en un fichero que incluye nombre y apellidos y Documento Nacional de Identidad y, por tanto, es susceptible de identificar a personas, (...) Desde luego, la finalidad perseguida mediante su utilización es plenamente legítima: el control del cumplimiento del horario de trabajo al que vienen obligados los empleados públicos. Y, en tanto esa obligación es inherente a la relación*

estos sistemas para el acceso al centro de trabajo cumple con la finalidad pretendida por el empresario, por lo que la medida es proporcional y el sistema establecido de control es lícito, ya que no existe norma que prohíba su utilización, justificando con este vacío normativo el recurso a cualquier medio de control horario que cumpla con las previsiones de la LOPD[996].

Respecto del cumplimiento del *principio de información*, cualquiera de estos medios habrán de asegurar que el titular del dato conozca de forma clara y concisa el tratamiento y uso que se le va a dar a la misma. Al igual que en todos los procesamientos de datos, el contenido de esta información debe ser acorde con lo establecido en el art. 5 de la LOPD, informando sobre la existencia del fichero; de su responsable; de los derechos de acceso, cancelación, rectificación y oposición; etc.

Más concretamente, y en relación con el uso de etiquetas de radiofrecuencia para supervisar la entrada de los trabajadores al centro de trabajo, hay que hacer referencia a lo establecido en el art. 7 de la Recomendación de la Comisión Europea, de 12 de mayo de 2009, sobre la aplicación de los principios relativos a la protección de datos y la intimidad en las aplicaciones basadas en la identificación por radiofrecuencia[997], que insta a los Estados para que velen porque las empresas encargadas de estos sistemas incluyan en las políticas sobre privacidad determinada información[998]

---

que une a estos con la Administración Autonómica, no es necesario obtener previamente su consentimiento ya que el artículo 6.2 de la Ley Orgánica 15/1999 lo excluye en estos casos. Además, no parece que la toma, en las condiciones expuestas, de una imagen de la mano incumpla las exigencias de su artículo 4.1. Por el contrario, puede considerarse adecuada, pertinente y no excesiva".

[996] GOÑI SEIN, J.L.: "Vulneración de derechos fundamentales en el trabajo…", op. cit., pp. 60-61; GOÑI SEÍN, J.L: "Controles empresariales: geolocalización…", op. cit., pp. 53-56; SELMA PENALVA, A.: "El control de accesos por medio de huella digital y sus repercusiones prácticas sobre el derecho a la intimidad de los trabajadores", *Revista Doctrinal Aranzadi Social*, núm. 2, 2010, pp. 3-5; DESDENTADO BONETE, A. Y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y…*, op. cit., pp. 107-108.

[997] DOUE L 122/47.

[998] Art. 7 de la Recomendación de 12 de mayo de 2009: "*Sin perjuicio de las obligaciones de los controladores de datos de conformidad con las Directivas 95/46/CE y 2002/58/CE, los Estados miembros deberían velar por que los operadores elaboren y publiquen una política de información concisa, exacta y fácil de comprender para cada una de sus aplicaciones. Dicha política debería incluir, como mínimo: a) la identidad y el domicilio de los operadores; b) la finalidad de la aplicación; c) los datos que procesa la aplicación, en particular si se trata de datos personales, y si se controla la localización de las etiquetas; d) un resumen de la*

para advertir sobre el tratamiento de datos contenido en estas aplicaciones informáticas.

Por su parte, la LOPD establece, de manera más matizada, que esta información tan solo podrá omitirse cuando, de la naturaleza del contenido de la relación laboral, se deduzca la finalidad de la recogida de datos personales, es decir, no será necesario informar de forma individual a los trabajadores de la instalación y posterior creación del fichero de datos cuando la medida se haya tomado con la única finalidad de verificar el cumplimiento por parte del trabajador de sus obligaciones, quedando constancia de este hecho con una información pública que pudiera concretarse en carteles informativos[999]. En estos carteles tan sólo se tiene que informar al trabajador de acerca de: la existencia de un fichero con la información captada a través del sistema de control y de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante, sin necesidad de hacerlo sobre el resto de aspectos contenido en el art. 5.1 de la LOPD.

La exigencia de información debe cumplirse a través de un medio que permita acreditar su realización, siendo en el ámbito laboral la forma más idónea de informar sobre estos aspectos, que tienen relación con la ejecución de la prestación de trabajo, la inclusión de un anexo en el propio contrato de trabajo. En la práctica, y como regla general, estas advertencias, relacionadas con la manera de controlar el acceso al centro de trabajo y la constitución de un fichero con los datos extraídos de ellos, no vienen explicitadas en el acuerdo laboral, informándose todo lo más, con carácter general, de la política de privacidad de la empresa, normalmente sita en su espacio web. Pero esta

---

evaluación del impacto sobre la protección de datos y la intimidad; e) los posibles riesgos para la intimidad, si existen, relacionados con el uso de etiquetas en la aplicación y las medidas que pueden adoptar las personas para reducirlos".

[999] La doctrina judicial también se ha pronunciado sobre este aspecto, en la Sentencia de la Audiencia Nacional de 4 de marzo de 2010 (JUR 2010/90775), en la misma se ampara la excepción al deber de información *"si del contenido de ella se deduce la naturaleza de los datos personales o de las circunstancias de la recogida"* (Art. 5.3 LOPD).

manera de advertir el tratamiento de datos no es suficiente, ya que no todos los trabajadores tienen la misma facilidad para la consultarla[1000]

Por su parte, la jurisprudencia ha admitido el derecho de los representantes de los trabajadores a ser informados por el empresario de no sólo de la utilización de estos medios de control sino del posterior tratamiento que pueda hacerse de esos datos de los trabajadores registrados en estos soportes. Obviamente, estos representantes de los trabajadores tiene que estar informados de los sistemas de control establecidos en la empresa[1001] para poder evitar, precisamente, que el trabajador se convierta en una persona demasiado transparente, obligando al empresario a indicar explícitamente el ejercicio de no sólo de esas actividades de control, sino del posterior tratamiento de datos que vaya a realizar a través de las tecnologías informáticas implantadas en su empresa, y que esa información será pertinentemente tratada y a qué efectos[1002].

[1000] Dependiendo del ámbito empresarial dónde desarrollen su actividad laboral tendrán más facilidad de acceder o no a su contenido, ya que éste puede estar más al alcance de un trabajador con labores administrativas o de gestión –con acceso a internet en el trabajo- que de un empleado que se dedique a trabajos en lo que gran parte de la jornada se encuentren fuera del centro de trabajo, por ejemplo, obras y reparaciones, trabajos agrícolas, etc.

[1001] Art. 64.5 del ET: *"El comité de empresa tendrá derecho a ser informado y consultado sobre la situación y estructura del empleo en la empresa o en el centro de trabajo, así como a ser informado trimestralmente sobre la evolución probable del mismo, incluyendo la consulta cuando se prevean cambios al respecto. Asimismo, tendrá derecho a ser informado y consultado sobre todas las decisiones de la empresa que pudieran provocar cambios relevantes en cuanto a la organización del trabajo y a los contratos de trabajo en la empresa. Igualmente tendrá derecho a ser informado y consultado sobre la adopción de eventuales medidas preventivas, especialmente en caso de riesgo para el empleo"* .Este aspecto está así contemplado, de forma más concreta en la citada Recomendación CM/Rec (2015) Comité de Ministros del Consejo de Europa sobre el tratamiento de datos personales en el contexto de empleo, de 1 de abril de 2015, ya que se hace necesario el consentimiento de los representantes de los trabajadores si se estima que estas medidas de control pueden vulnerar los derechos y libertades fundamentales de los trabajadores (apartado 21. c). De esta forma, se le otorga un papel primordial a estos representantes convirtiéndose en instrumentos de fiscalización previa a la actuación de los empleadores en el ámbito de control y vigilancia. Lógicamente, esta apreciación se traslada a cualquier mecanismo de control que se haga al trabajador en el marco empresarial – videovigilancia, correo electrónico, ordenador, sistemas de acceso, etc.-

[1002] Sentencia de la Audiencia Nacional 74/2005 de 12 de julio (AS 2005\2674): *"Por lo que respecta a la pretensión b), relativa a «...la obligación de comunicar a los representantes de los trabajadores el funcionamiento del sistema de control horario para que puedan constatar el correcto funcionamiento del mismo...», solo cabe señalar para su desestimación, de un lado, que tal comunicación para la constatación del funcionamiento correcto del sistema de control horario se llevó a cabo, entrando, además, dentro de las tareas generales de vigilancia de tales representantes –artículos 62, 64 y concordantes del Estatuto de 1995 y de igual contenido normativo de la Ley Orgánica de Libertad Sindical de 2 de agosto de 1985 (RCL 1985, 1980) – la labor de fiscalizar los aparatos marcadores de tal tipo, sin que conste que a ello se haya*

Ya se ha afirmado de forma reiterada que el *consentimiento* del trabajador para un tratamiento de datos que tenga como objetivo el mantenimiento o cumplimiento de una relación laboral, no es necesario ya que ese tratamiento vendría amparado por lo previsto en el art. 6.2 de la LOPD. Como se ha dicho ya , esta excepción tiene su fundamento en la existencia de un consentimiento previo, otorgado antes de iniciarse la relación laboral, es decir, en la firma del contrato de trabajo, y también en la habilitación legislativa impuesta por lo establecido en el art. 20.3 del ET[1003]. Ello, obviamente, con independencia de la obligación del empresario de informar al trabajador de todo lo relativo al tratamiento de datos recogidos en los sistemas de control de acceso, ya que es claro que la excepción al consentimiento no implica la inobservancia del principio de información regulado en el art. 5 de la LOPD[1004].

Cosa distinta ocurre si, por ejemplo, esos datos son registrados a través de sistemas biométricos y, como consecuencia de su tramitación, se desvelen aspectos relacionados con la salud del trabajador, los cuáles se generan con el simple análisis del iris. Puesto que el problema que presenta la lectura biométrica es la posibilidad de que un simple control de cumplimiento del horario de trabajo llegue a revelar aspectos privados que el empresario no está habilitado a tratar ni siquiera en ejercicio de las facultades del art. 20.3 ET, cualquier procesamiento de esa información requiere el consentimiento expreso del trabajador en cuestión.

3.3.2. Sistemas de videovigilancia y protección de datos del trabajador.

La videovigilancia es un sistema concebido inicialmente para la finalidad de garantizar la seguridad y prevención de cualquier delito en la empresa. Sin embargo, además de tener este objetivo puede configurarse como un

---

negado la empresa, y de otro lado, que ningún derecho más al respecto deriva de lo prevenido en el artículo 35.3 estatutario, en la adicional tercera reglamentaria, en el Pacto de 1991 y en la normativa del mismo derivada".

[1003] Vid., Informe 193/2008 de la AEPD, disponible en http://www.agpd.es/portalwebAGPD /canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2008-0193_Tratamiento-de-datos-de-GPS-en-veh-ii-culos.pdf. [Consulta 5/05/2015].

[1004] GOÑISEÍN, J.L.: "Vulneración de derechos fundamentales…", op cit., pp. 58-60; TRONCOSO REIGADA, A: "Libertad sindical, libertad de empresa y derecho a la intimidad y a la protección de datos de los trabajadores" en FARRIOLS I SOLA, A. (coord.): *La protección de datos de carácter personal en los centros de trabajo*, Ediciones Cinca, 2006, pp.136-138.

mecanismo de control de la prestación de trabajo. Si así fuera, el empresario a través de la captación de imágenes de los trabajadores puede obtener una amplia e incontrovertible información personal con posibles consecuencias laborales.

En la captación de imágenes en los centros de trabajo es habitual que se produzca la identificación de los trabajadores o, incluso, de terceras personas ajenas a la empresa que también acceden a los lugares de trabajo donde están instaladas las cámaras. Una vez que con la imagen se ha podido identificar claramente a la persona, en este caso al trabajador, hay que recordar que, para que exista tratamiento de ese dato captado por la cámara, éste debe ser almacenado en un fichero estructurado[1005] o que se produzcan algunas de las actuaciones tasadas en el art. 3 c) de la LOPD relacionadas con la recogida, grabación, cesiones de imágenes de empresas de vigilancia al empleador, cancelaciones etc.[1006].

Antes que nada es preciso tener en cuenta las distintas formas en las que se puede invadir los derechos de la personalidad de los trabajadores, siendo la menos agresiva de todas aquélla en la cual las imágenes se envían directamente a la pantalla de un monitor en el que no es posible ni la transmisión ni el almacenamiento de las grabaciones, no pudiendo considerarse en este supuesto una violación del derecho a la protección de datos ya que lo que se hace es simplemente visualizar la imagen[1007]. Por el contrario, en los casos en que las cámaras sí permiten realizar estas operaciones, el empresario puede efectuar un aprovechamiento de las imágenes durante más tiempo. Los recursos técnicos de estos instrumentos son

[1005] Según la AEPD: *"El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas*", vid., Instrucción 1/2006 de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras (BOE núm. 296 de 12 de diciembre de 2006).
[1006] Sin embargo, la jurisprudencia ha sancionado, en ocasiones y contradiciendo lo establecido en la Instrucción 1/2006, el volcado de imágenes en un servidor de internet de la empresa sin que se almacenaran o grabaran en ningún fichero, ya que establece que no cabe duda de que la emisión de imágenes a través de internet constituye una cesión de datos y, por tanto, un tratamiento (Sentencia de la Audiencia Nacional de 24 de enero de 2003, JUR 2006\275817).
[1007] Sobre este aspecto la jurisprudencia ha establecido que …

también un factor a tener en cuenta, ya que, cuanto más completo sea el equipamiento electrónico, más grave será el ataque al derecho a la protección de datos, sin perjuicio de que a través de un *software* adecuado se pueda limitar de forma automática la vigilancia o dejar ocultos ciertos espacios de la empresa[1008].

En todo caso, esta información se puede llegar a almacenar en ficheros cuya responsabilidad la ostenta el empresario; siendo obviamente necesario establecer que efectivamente, la imagen constituye un dato de carácter personal[1009], lo que parece indiscutible. Partiendo de este hecho, se trata ahora de establecer las obligaciones empresariales al respecto en respeto de las exigencias de las normas que rigen la protección de datos.

En primer lugar, el almacenamiento de esas imágenes debe responder a una única finalidad legítima y no utilizarse con otro objetivo, por lo que el empresario debe acreditar lo que pretende con el registro de ese dato. Por ejemplo, probar un supuesto incumplimiento contractual; velar por la seguridad de su empresa; o detectar un posible uso indebido de los instrumentos de trabajo. En razón de lo anterior, cualquier utilización no acordada y

[1008] GUDE FERNÁNDEZ, A.: "La video vigilancia laboral y el derecho a la protección de datos de carácter personal", *Revista de Derecho Político*, núm. 91, 2014, pp. 46-48; DESDENTADO BONETE, A. Y MUÑOZ RUIZ, B.: "Trabajo, video vigilancia y controles informáticos. un recorrido por la jurisprudencia" *Revista General de Derecho del Trabajo y de la Seguridad Social,* núm.39, 2014, pp.12-17;VIDAL, P.: "La utilización de las cámaras de video vigilancia para fines disciplinarios y de control del trabajo." *Actualidad Jurídica Aranzadi*, núm. 888, 2014.

[1009] En lo relativo a la imagen la normativa sobre protección de datos ha establecido como criterio genérico la calificación de dato personal de todas aquellas informaciones que identifiquen claramente a una persona (Art. 3 a) de la LOPD) y, además en el RDLOPD se hace alusión a la imagen cuando en su art. 5 define lo que se considera dato de carácter personal: "*Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"*. También la AEPD ha aclarado que la imagen se considera dato de carácter personal, vid., Informe jurídico 624/2006, disponible en https://www.agpd.es/ portalwebAGPD/ canal documentacion/informes juridicos/cesiondatos/common /pdfs/2009-0624_Publicaci-oo-n-en-revista-de-foto-ganadora-de-concurso-con-im-aa-genes-de-personas.-No-necesidad-de-con sentimiento.pdf. [Consulta 20/03/2015] e Informe jurídico 424/2009, disponible en https:// www.agpd.es/portalwebAGPD/canaldocumentación/informesjurídicos/conceptos/common/pdfs/ 2009-0424Tratamiento-de-los-fotografos-por-motivos-excepcionales.pdf [Consulta 20 /03/2015]. Lo mismo concluye el grupo del art. 29 en su Dictamen 4/2004, adoptado el 11 de febrero de 2004, disponible en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89 _es.pdf, pp. 15-16. [Consulta 12/10/2015], cuando establece que las imágenes son consideradas datos de carácter personal aunque no estén asociadas a la información personal de los interesados.

desconocida por el titular del dato iría contra el *principio de calidad* en el tratamiento de datos.

Obviamente, el empresario tendrá que advertir, de forma general, no sólo de la existencia de las cámaras sino también de la posibilidad de que esas imágenes sean grabadas[1010], cumpliendo de esta manera lo establecido en art. 5.1 de la LOPD respecto del *principio de información*. Aun así, en el terreno laboral, además de la advertencia de la existencia de cámaras se tiene que informar a los trabajadores del destino que se le va a dar a esas grabaciones y de su verdadero objetivo para no enmascarar con las acciones relacionadas con la seguridad del centro de trabajo otras pretensiones que tenga el empresario relacionadas con la vigilancia de la actividad laboral[1011].

Sobre este aspecto hay distintos criterios jurisprudenciales, ya que en ocasiones se ha admitido la falta de información previa a los trabajadores sobre la existencia de las cámaras, justificando este hecho en la pérdida de efectividad de la medida si se hubiera avisado a los trabajadores de su instalación[1012]. En realidad, esta dispensa del principio de información[1013]

[1010] La instalación de estas videocámaras implica la obligación de exponer en las zonas contraladas un distintivo informativo bien visible, cuyo uso y exhibición son obligatorios a tenor de lo establecido en la citada Instrucción 1/2006 de la AEPD.

[1011] Véase Sentencia del Tribunal Supremo de 13 de mayo de 2014 (RJ\2014\3307) en la que no se admite la grabación de imágenes como prueba para justificar el despido de la trabajadora pues, aunque ésta conocía la existencia de las cámaras, no sabía la finalidad pretendida por el empresario con esas filmaciones, ya que pensaba, al igual que la representación de los trabajadores, que el objetivo de la grabación estaba relacionado con la intención de disuadir a los clientes ante posibles hurtos. El Supremo sigue con esta Sentencia la misma línea jurisprudencial que había mantenido el Tribunal Constitucional en su Sentencia 29/2013, de 11 de febrero (RTC 2013\29).

[1012] Fundamento Jurídico Siete de la Sentencia 186/2000, de 10 de julio: *"El hecho de que la instalación del circuito cerrado de televisión no fuera previamente puesta en conocimiento del Comité de empresa y de los trabajadores afectados (sin duda por el justificado temor de la empresa de que el conocimiento de la existencia del sistema de filmación frustraría la finalidad apetecida) carece de trascendencia desde la perspectiva constitucional, pues, fuese o no exigible el informe previo del Comité de empresa a la luz del art. 64.1.3 d) LET, estaríamos en todo caso ante una cuestión de mera legalidad ordinaria, ajena por completo al objeto del recurso de amparo. Todo ello sin perjuicio de dejar constancia de que los órganos judiciales han dado una respuesta negativa a esta cuestión, respuesta que no cabe tildar de arbitraria o irrazonable, lo que veda en cualquier caso su revisión en esta sede".*

[1013]Sobre este aspecto la AEPD ha admitido la posibilidad de grabar imágenes sin información previa justificando este hecho en la proporcionalidad de la medida ante la evidencia, de alguna incidencia anterior, sobre conductas impropias de los trabajadores, vid., Resolución 681/2004 de la AEPD, disponible en http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2004/common/pdfs/PS-00109-2004_Resolucion-de-fecha-10-12-2004_Art-ii-

parece justificarse esencialmente respecto de controles en situaciones en las que han existido infracciones laborales relevantes y sea necesario investigar, siempre que concurra alguna sospecha sobre la irregularidad de la conducta del trabajador, sin que este argumento pueda generalizarse para la instalación, sin información previa, de cualquier cámara de videovigilancia en la empresa[1014].

Por ello, es importante tener en cuenta el extenso voto particular de la Sentencia 39/2016 del Tribunal Constitucional de 3 de marzo de 2016[1015], ya que muestra su disconformidad con la Sentencia de referencia al apartarse sin justificación alguna de la línea establecida en la citada Sentencia 29/2013 del TC[1016], por considerar conforme a derecho el tratamiento de datos efectuado por el empresario de las imágenes captadas por las cámaras de videovigilancia, sin que quede constancia de que se haya dado información

culo-5.1-LOPD.pdf.[Consulta 21/03/2015]. Sin embargo, hay otras ocasiones en las que no se admite la captación y almacenamiento de imágenes sin advertir de esta actuación al trabajador, vid., Resolución 1823/2008 de la AEPD, disponible en http://www.agpd.es/portalwebAGPD/ resoluciones/procedimientos_sancionadores/ps_2009/common/pdfs/PS-00519-2008.

[1014] Así lo ha previsto la AEPD cuando establece que: *"En el caso que nos ocupa, ha quedado acreditado que no existían carteles informativos en el establecimiento que advirtieran de la instalación de las cámaras de videovigilancia. A mayor abundamiento, de conformidad con la alegación de Dña. G.G.G., en representación de MERCADONA, S.A., esta manifiesta que haber instalado un cartel informando de la existencia de la cámara hubiera frustrado la finalidad legítima para la que se instaló. Por tanto, puesto que la información en la recogida de los datos es un elemento esencial del derecho a la protección de datos y su cumplimiento resulta ineludible, MERCADONA, S.A. al no informar a sus trabajadores de centro ubicado en Ferrol, y a cualquier afectado, de la instalación de las dos cámaras de videovigilancia ha incumplido con el deber de información impuesto por el artículo 5.1 de la LOPD en relación con el artículo 3 de la Instrucción 1/2006, de la Instrucción 1/2006, de 8/11, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras"*. Vid., R/01414/2009, disponible en http://www .agpd.es/portalwebAGPD/resoluciones/procedimientossancionadores/ps_2009 /common/pdfs/ PS-00126-2009_Resolucion-de-fecha-10-06-2009_Art-ii-culo-5-LOPD.pdf. [Consulta 05/05/ 2015].

[1015] RTC 2016\39.

[1016] La Sentencia 29/2013 del TC declara nula una sentencia que había declarado procedente un despido por transgresión de la buena fe contractual, por el simple hecho que si bien el trabajador había incumplido sus obligaciones laborales de una forma clara, flagrante y reiterada, y así se había podido acreditar a través de los dispositivos de video vigilancia instalados en la empresa con la finalidad de efectuar controles de seguridad en sus accesos y perímetro, al constatarse que al trabajador ni en el momento de ser contratado ni en un momento posterior no se le había informado de forma previa y expresa, clara e inequívoca de la finalidad de control de la actividad laboral que podían tener los dispositivos de captación de imágenes. Por lo que La STC 29/2013 establece la doctrina de que el deber de información vinculado a la instalación de cámaras de vigilancia en el establecimiento laboral debe ir acompañada de información a los trabajadores sobre la finalidad de control de la actividad laboral.

concreta al trabajador sobre el procesamiento de esos datos. Por lo que el análisis del voto particular, de la Sentencia 39/2016, se puede resumir en los siguientes puntos: a) Utilización del juicio de proporcionalidad para no darle importancia al contenido esencial del derecho a la protección de datos, justificando esta situación en la posible licitud de la medida de vigilancia al trabajador; b) Entender que existe el derecho de información a los trabajadores sobre la captación y posterior uso de sus datos personales, cuando no se ha informado de forma precisa al trabajador en concreto; c) Primacía de los intereses empresariales ante los derechos fundamentales de los trabajadores, entre el que se encuentra el derecho a la protección de datos.

Sobre la exigencia o no de solicitar e consentimiento del trabajador al tratamiento de las imágenes se puede decir que la grabación del trabajador en su puesto de trabajo se realiza con el objetivo de mantener la relación de trabajo y, éste consentimiento, como se ha repetido, puede considerarse implícito en la aceptación del contrato de trabajo.. Ahora bien, si la acción empresarial va más allá del control de la actividad profesional, por ejemplo, difundiendo imágenes de los trabajadores por internet con la intención de reflejar la actividad y el movimiento de los trabajadores, no estaría dentro del ámbito de la excepción al consentimiento, puesto que esta actuación no puede confundirse con el control de la prestación de trabajo y, por tanto, el sostenimiento del contrato de trabajo[1017].

En los casos en los que sea necesario el consentimiento de los trabajadores se rechaza la posibilidad de que éste sea tácito, basado en la inactividad de los trabajadores ante la implantación del sistema de videovigilancia ya que puede ser una actitud propiciada, precisamente, por la falta de información sobre la instalación del sistema. Es decir, el hecho de no hacer nada en contra de estos medios de control no permite afirmar que se

[1017] AEPD: Guía sobre videovigilancia, 2008, pp. 34-35, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentación/publicaciones/common/pdfs/guia_videovigilancia.pdf. [Consulta 05/05/2015].

esté de acuerdo con ellos, ya que puede ser que ni siquiera se conozca su existencia[1018].

3.3.3. Detectives privados como medio de vigilancia del cumplimiento de la prestación de trabajo y tratamiento de datos.

Atendiendo a la vigilancia que puede ejercer el empresario aparece también la figura del detective privado, contratado para supervisar la actividad del trabajador dentro o fuera del centro de trabajo, ya que en ocasiones es preciso efectuar el control empresarial más allá de los límites de la propia empresa[1019]. Así sucede cuando se trata de fiscalizar la actividad laboral de los trabajadores cuando éstos desarrollan su actividad fuera del establecimiento empresarial (representantes de comercio, montadores, instaladores, vendedores a domicilio, transportistas, etc.); cuando se sospecha que el trabajador realiza actividades de concurrencia ilícitas, por cuenta propia o por cuenta ajena; cuando es necesario verificar las causas de inasistencia o de puntualidad alegadas por el trabajador, y comprobar eventuales incumplimientos laborales; y en los casos en que se trata de fiscalizar ciertas conductas extra laborales, contrarias al deber de buena fe, de trabajadores en situación de incapacidad temporal, o con contrato suspendido por otras causas[1020]. Actuaciones de control que una numerosa jurisprudencia[1021] ha avalado. ,

---

[1018] Sobre el consentimiento del trabajador afectado vid., GOÑISEÍN, J.L.:*La videovigilancia empresarial y la protección de datos personales*, Thomson-Civitas, 2007, pp. 95-103.

[1019] Existe una corriente doctrinal a favor de la contratación de detectives privados para controlar al trabajador DEL VALLE VILLAR, J.M.: "El derecho a la intimidad del trabajador durante la relación de trabajo"…pp. 494-495; y otra en contra de esta postura GOÑISEÍN, J.L.: *El respeto a la esfera privada del trabajador*…, op. cit., pp. 134-138.

[1020] LÓPEZ ANIORTE, M.C.: "Límites constitucionales al ejercicio del poder directivo empresarial mediante el uso de las TIC y otros medios de vigilancia y seguridad privada en el ordenamiento jurídico español", *Policía y Seguridad Pública,* vol.1, núm. 4, 2014, pág.44; MATEU CARRUANA, M.J.: "Facultades de control fuera del centro de trabajo: medidas de control sobre las conductas extralaborales del trabajador"*, Tribuna Social*, núm. 169, 2005, pp. 41 y ss.; AGUILERA IZQUIERDO, R.: "*El ejercicio de las facultades de vigilancia y control por el empresario a través de agencias de detectives,* Revista Española de Derecho del Trabajo, núm. 158, 2013, pp. 136 y ss.

[1021] Así, el primer pronunciamiento judicial sobre este asunto fue la Sentencia del Tribunal Supremo de 19 de julio de 1989 (RJ 1989\5878), aunque la admisión de este tipo de vigilancia estaba relacionada con la naturaleza de la prestación de servicios encomendada al trabajador, por lo que su utilización era excepcional o extraordinario y sólo se podía recurrir a ella cuando no fuera posible controlar al trabajador de otra forma. A ésta le siguieron otras resoluciones judiciales como: Sentencia del TSJ Cataluña del 13 de mayo de 2005 (JUR 2005\169963) que contempla el supuesto de un viajante de industria cárnica que es despedido por incumplir

Naturalmente, el detective privado maneja datos de carácter personal de los trabajadores y además la manipulación de esa información la realiza, incluso, antes de iniciar su labor investigadora ya que el empresario, cuando establece la relación de servicios con el investigador, tiene que facilitarle a éste datos identificativos del trabajador que va a ser sometido a seguimiento. De forma que ya esta comunicación de datos del empresario al detective debe estar rodeada de las garantías que la LOPD otorga a la cesión de datos de carácter personal. En consecuencia, el empresario deberá limitarse a comunicar la información relativa a las tareas del trabajador y sus circunstancias laborales.

Ciertamente, el trabajador puede no ser conocedor de la utilidad que el empresario está dándole en este caso a sus datos personales y con qué fines realiza la citada cesión, ya que no tiene ninguna información acerca de la realización de este tipo de control. Por lo que, en un primer momento, esta actuación podría ser contraria al *principio de calidad* por usar esa información para fines incompatibles con la razón que motivó su recogida -firma del contrato de trabajo- y también contra el *principio de información* ya que no se le ha informado al trabajador, si es el caso, de las posibles comunicaciones de datos a terceros con el objeto de controlar la prestación de trabajo. En consecuencia, parece necesario que para la cesión inicial de datos del empresario al detective, el primero tenga la habilitación del trabajador para hacerlo, habiendo aceptado la cesión de datos a terceros para finalidades laborales o relacionadas con la prestación de trabajo.

Acerca del *consentimiento* para tratar esas informaciones, es necesario apreciar que el trabajador tan sólo consiente el almacenamiento de sus datos en los ficheros empresariales para mantener y controlar su prestación de trabajo. Por tanto, si se atiende a lo establecido en la LOPD, la excepción del

---

reiteradamente su jornada laboral, lo que se acredita mediante prueba la testifical de un detective que informa de la realización por aquél, durante la jornada laboral, de diversas actividades distintas al desarrollo del trabajo comprometido. El órgano judicial califica el despido como procedente, y considera válida la prueba testifical del detective. En parecidos términos vid., Sentencia del TSJ de Castilla la Mancha de 21 de mayo de 2003 (AS 2003\2920).

consentimiento para la cesión de datos a un tercero no podría darse ya que, ni está prevista en una norma, ni es necesaria para colaborar en las tareas del cedente[1022]. Evidentemente, esta cesión no es necesaria para cumplir con el objetivo de procurar el mantenimiento de la relación contractual, sino más bien para que un investigador, ajeno a la empresa, ejerza el poder de control sobre los trabajadores.

En todo caso, el consentimiento obligatorio del trabajador a la cesión solamente podría quedar excepcionado si el control de ese trabajador, a través de este medio, fuera imprescindible para asegurar el buen desarrollo de la actividad del empresario (cedente del dato del trabajador). Por ejemplo, si la cesión de datos se justifica en la necesidad del empresario de conocer y registrar los movimientos del trabajador para comprobar así el cumplimiento de la relación de trabajo, Obviamente, en estos casos no tiene sentido que el empresario le pidiera autorización al trabajador para ceder los datos al detective privado, ya que, si así fuera, el control no podría realizarse o se desvirtuaría la finalidad de la vigilancia pues el trabajador actuará de forma distinta si sabe que va a ser observado por un investigador privado contratado por la empresa.

De otra parte, cuando el investigador privado termina su labor el problema radica ahora que tiene en su poder una gran cantidad de información de los trabajadores que será archivada en los pertinentes ficheros informáticos. . Sin duda, el detective privado pasa ahora a ser responsable de este fichero con los datos obtenidos como consecuencia del seguimiento realizado a los trabajadores y, por tanto, es el encargado de velar por él respetando para ello, los principios de la LOPD. Por este motivo, el investigador tendrá que hacer un uso de los datos compatible con la finalidad que ha generado su almacenamiento, es decir, no podrá utilizar o comunicar al empresario otras informaciones que excedan del objeto de la investigación[1023]que no es otro que

[1022] Ver art. 11 de la LOPD y analizar las distintas excepciones.

comprobar si ese trabajador está realizando su trabajo diligentemente[1024]. En consecuencia, deberá limitarse a comunicar al empresario y a tratar informáticamente todo lo relativo a l cumplimiento por parte del trabajador de sus obligaciones laborales, sin hacer otras observaciones ni siquiera comunicar y tratar aquellas otras apreciaciones superfluas relacionadas con las actividades, aficiones o intereses de los trabajadores que se pueden obtener cuando el investigador privado hace un seguimiento del empleado en la calle y que no tienen por qué ser conocidas por la empresa.

Aunque es hoy admitido el uso de este medio de supervisión de los trabajadores, la utilización de este instrumento puede ser intrusivo para el derecho a la protección de datos, puesto que el trabajador no tiene conocimiento del manejo de sus datos identificativos por parte de un detective privado ni del posible almacenamiento de la información generada con el seguimiento que le hace este investigador privado contratado por el empresario. Por lo que en estos supuestos ni ha consentido el tratamiento de sus datos ni ha sido informado acerca de esa base de datos, produciéndose una pérdida de control de su información personal, recabada ahora por ese investigador privado.

Acordado que el empresario puede llegar a contratar a un investigador privado si tiene sospechas acerca de la falta de actividad de sus empleados, éste tendría que ser responsable de esa información y tratarla con la diligencia debida para no atentar el derecho a la protección de datos, ya que éste sÍi puede procesar esta información que le transmite el detective de acuerdo con

[1024] Análogamente vid., la Sentencia del TSJ del País Vasco de 10 de mayo de 2011 (AS 2012\2277), contiene un ejemplo de injerencia desproporcionada en el derecho a la intimidad por parte de un investigador privado, que coloca un dispositivo de localización GPS en el vehículo privado del demandante, sin su conocimiento ni autorización, y sin que concurrieran circunstancias que justificaran su instalación, para comprobar la posible realización de actividades incompatibles con su situación de incapacidad temporal. Ello supone, a juicio del órgano judicial, la vulneración del "derecho a no estar localizado de manera continua por medios electrónicos colocados en sus bienes contra su voluntad" durante el día y la noche. No se considera una medida equilibrada puesto que, de la misma, no se derivan más beneficios para el interés empresarial que perjuicios sobre el derecho a la intimidad. Se entiende que habría sido un mecanismo adecuado, por ser menos intrusivo, la vigilancia directa por el vigilante. Este supuesto se puede trasladar a uso de los datos captados por ese GPS, ya que se llega a obtener más información del trabajador que la necesaria para realizar un efectivo control de la relación de trabajo.

lo establecido en el art. 20.3 del ET y ante la desconfianza generada con esos trabajadores determinados. Por tanto, el detective deberá borrar toda la información de ese trabajador investigado una vez que termine la tarea para la que ha sido contratado por el empresario, eliminando de esta manera cualquier vestigio de ese empleado en sus bases de datos.

3.3.4. Sistema de denuncias internas: "Whistlebowling".

Los sistemas de denuncia interna en las empresas o *whistleblowing*[1025] son los referidos a la creación de un buzón online en la empresa para denunciar posibles incumplimientos por parte de los empleados. Por medio de este instrumento se pretende vigilar también las irregularidades en la prestación de trabajo, incentivando denuncia anónimas de [1026]comportamientos, incluidos directivos de la misma, contrarios a las obligaciones laborales o a las normas de conducta de la empresa, recogidas en sus Códigos de Conducta, estableciéndose en todo caso, los procedimientos necesarios para garantizar la confidencialidad del denunciante cuya identidad no debe ser comunicada al denunciado[1027].

Si con la captación de esta información se crea un fichero con información personal de los trabajadores denunciados, se está realizando sin duda un tratamiento de datos de carácter personal cuyo acceso está limitado al empresario que lo instala, que será, a su vez, el responsable de esa base de datos. No obstante, además del procesamiento de datos automatizados,

[1025] La palabra inglesa *whistleblower* no tiene traducción literal al castellano. Lo más cercano sería algo parecido a chivato, delator, soplón institucional, términos que otorgan una connotación muy despectiva de la función que realmente se realiza. Hace referencia al toque de silbato que realiza un policía inglés cuando observa una conducta inapropiada e interpela al infractor mientras lo persigue para que sus compañeros se unan a la persecución y los transeúntes sean conscientes del peligro.

[1026] Sobre este aspecto la Recomendación CM/Rec (2015) Comité de Ministros del Consejo de Europa sobre el tratamiento de datos personales en el contexto de empleo, de 1 de abril de 2015 acepta, aunque con limitaciones, el que se interpongan denuncias de manera confidencial para asegurar la veracidad del proceso y el éxito de la investigación subsiguiente.

[1027] No obstante, no es un sistema muy extendido en España aunque está alcanzado cada vez más repercusión entre las empresas cotizadas en bolsa. El Congreso de los Estados Unidos aprobó en el 30 de Julio de 2002 la Ley Sabarnes-Oxey de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista (en adelante,SOX)15 (*Pub. L. No. 107-204, 116 Stat. 745)*. La SOX surgió en respuesta a varios escándalos financieros como el de Enron y Worldcom que afectaron a la economía Americana y provocaron una pérdida de confianza en el sistema financiero, y en especial, en los procedimientos contables y de auditoria a los que se sometían las sociedades estadounidenses cotizadas en bolsa.

proveniente de la denuncia online, puede ocurrir que el denunciante presente una queja por escrito ante la persona responsable en la empresa de tramitar este sistema interno de denuncias. Como es sabido, y teniendo en cuenta la doctrina de la Audiencia Nacional[1028], la LOPD es aplicable a cualquier fichero manual que se pueda constituir, por lo que también se considera tratamiento de datos el hecho de incluir la información del trabajador en un archivo físico y no automatizado.

Una vez verificado que existe tratamiento de datos con la interposición de denuncias a través del sistema interno de la empresa, hay tratar la posible colisión del derecho a la protección de datos de carácter personal de los trabajadores que puede producirse con la notificación y el tratamiento de sus datos por este medio, siendo necesario acudir a lo establecido en la normativa sobre protección de datos y a los informes u opiniones derivados de la aplicación de la LOPD. Como resultado del análisis de estas medidas de control, la AEPD ha redactado un informe jurídico como consecuencia de una consulta realizada por una empresa farmacéutica en la que solicita su colaboración para certificar que la creación de un sistema de denuncias internas en su empresa es conforme a la normativa sobre protección de datos. Entre otras cuestiones, el citado informe de la AEPD permite la creación de un canal de denuncia siempre que las personas cuyos datos podrían ser tratados,

[1028] Sentencia de la Audiencia Nacional de 19 de mayo de 2004 (JUR 2004\253765): *"La tesis en cuyo favor pugna la actora se conduce porque los datos de carácter personal contenidos en ficheros no automatizados, pueden ser comunicados libremente a terceros durante un plazo de doce años, que es el establecido en la LOPD para su adecuación a la Ley, lo que supondría la quiebra consiguiente de todo el sistema de protección de los derechos de las personas. Es por ello que las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, que garantizan y protegen, en lo concerniente al tratamiento de los datos personales, los derechos fundamentales y las libertades públicas de la personas físicas y, especialmente, su derecho al honor y a la intimidad personal y familiar, han de aplicarse inmediatamente, en virtud del principio de aplicabilidad inmediata de los derechos fundamentales, según doctrina del Tribunal Constitucional recogida en la Sentencia 81/1992, de 28 de mayo. En consecuencia, los plazos que prevé la Disposición Adicional Primera, de la citada Ley para la adecuación de los ficheros y tratamientos automatizados y no automatizados de datos, no se considera referido a las aludidas previsiones. Efectivamente, las previsiones sustantivas de la LOPD tienen por objeto la protección de las libertades públicas y los derechos fundamentales de las personas físicas y, más particularmente, la protección del derecho al honor y a la intimidad personal y familiar; así resulta del artículo 1 de la LOPD que, en consonancia con el artículo 1 de la Directiva 95/46/CE dispone que "La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".*

trabajadores en este caso, conocieran su existencia y que el tratamiento de esa información fuera necesario para el desarrollo y control adecuado de la relación contractual. Adicionalmente, la AEPD no respalda el criterio sobre la conservación de las denuncias como anónimas, incentivando que se evite la presencia garantizando así la exactitud e integridad de la información contenida en dichos sistemas de denuncias[1029].

Con anterioridad a este informe, en el seno de la UE, el Grupo de Trabajo del art. 29 ya había adoptado en el Documento WP 117, la Opinión 1/2006[1030], en la que se establecían las exigencias que tenían que cumplir los programas de denuncias internas para ser compatibles con la normativa sobre protección de datos de carácter personal –legitimidad de los sistemas, aplicación de los principios de calidad y proporcionalidad de los datos, información clara y completa sobre el uso y gestión del sistema, medidas de seguridad, derechos de las personas incriminadas, etc.-

Ciertamente, cuando se producen denuncias sobre determinados comportamientos de los trabajadores relacionadas con el incumplimiento de las normas que regulan su actividad o conducta dentro de la empresa, estos datos se tienen que utilizar atendiendo al *principio de calidad* en el tratamiento de datos, respetando la finalidad que propició la recogida de su información personal y tan sólo durante el tiempo necesario para cumplir con el objetivo empresarial pretendido[1031] (controlar el cumplimiento de las normas internas por parte del trabajador). Además, el empresario al tratar estas informaciones

[1029] Para un mayor abundamiento sobre la cuestión de referencia vid., Informe jurídico 128/2007 de la AEPD, disponible en http://www.agpd.es/portalwebAGPD/ canaldocumentación/informes jurídicos/otras_cuestiones/common/pdfs/2007-0128_Creaci-oo-n-de-sistemas-de-denuncias-internas-en-las-empresas-mecanismos-de-whistleblowing.pdf. [Consulta 23/08/2015].

[1030] Documento WP 117 del Grupo del Art. 29, adoptado el 1 de febrero de 2006, disponible en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_es.pdf. [Consulta 23/08/ 2015].

[1031] Según Álvarez Hernando, J.: "Debe establecerse un plazo máximo para la conservación de los datos relacionados con las denuncias, a fin de evitar su mantenimiento por un período superior que perjudique los derechos del denunciado y del propio denunciante, cuya confidencialidad debe quedar garantizada. Este plazo debería limitarse a la tramitación de las medidas de auditoría interna que resultasen necesarias y, como máximo, a la tramitación de los procedimientos judiciales que se derivasen de la investigación realizada" en "Relaciones laborales y protección de datos", Practicum Protección de Datos 2015, Aranzadi, 2014, pp. 39-41.

captadas a través de este sistema de denuncias debe respetar siempre el principio de proporcionalidad, es decir, no podrá almacenar más informaciones que las realmente imprescindibles y no excesivos para describir el hecho y la persona denunciada, que haya infringido la ley o las normas de conducta de la empresa.

Al tratarse de un ámbito muy delicado, el deber de *información* al empleado acerca de la existencia de este tipo de sistemas de denuncias ha de hacerse mediante circulares de la empresa o bien con la firma de una normativa de confidencialidad anexa al contrato de trabajo, explicitando el tratamiento de datos que se va a realizar con la información recogida por ese sistema. También se puede comunicar su existencia en el tablón de anuncios de la empresa, ya sea éste "físico" o virtual.

Sobre el *consentimiento* se puede decir que cabe la excepción al mismo establecida en el art. 6.2 de la LOPD, ya que el empresario pretende supervisar el cumplimiento de las normas e, indirectamente, el del contrato de trabajo. Ahora bien, esta excepción se aplicará solamente a aquellos casos en los que previamente se le haya informado al trabajador de la existencia de estos instrumentos y del control que va a ejercer el empresario a través de ellos[1032].

En cuanto a la cesión de los datos de carácter personal, en aquellos supuestos en los que la administración del sistema de denuncias se externaliza, tanto el denunciante como el denunciado deberán ser debidamente informados incluyendo la posible transferencia internacional de datos a otras empresas, si se tratara de un grupo de empresas con presencia internacional.

Del mismo modo, el trabajador acusado debe poder ejercer su derecho de rectificación, cancelación y oposición ante el fichero que se ha creado en la empresa con esa información pudiendo conocer los datos que han motivado la denuncia, con el fin de poder defenderse. Al igual que ocurre con cualquier

[1032]SAMPEDRO BURGOS, G.: "Reflexiones sobre la aplicación de la normativa de protección de datos en el ámbito del control del empresario y sistemas de denuncias internas",*Revista General de Derecho del Trabajo y de la Seguridad Social,* núm. 26, 2011, pp. 135-144.

base de datos de carácter personal, estos ficheros configurados con este objetivo deberán ser notificados al Registro General de la Agencia de Protección de Datos[1033].

4. CRITERIOS DE CANCELACIÓN DE DATOS EN LA EXTINCIÓN DEL CONTRATO DE TRABAJO.

Como es sabido, la normativa sobre protección de datos personales habilita a los ciudadanos, en este caso trabajadores, para poder ejercitar una serie de derechos ante el responsable del fichero, en lo que aquí interesa, empresario[1034]. Entre estos derechos se encuentra la cancelación de los datos, cuya aplicación alcanza su mayor grado de implantación en la empresa cuando se ha extinguido la relación de trabajo entre empresario y trabajador.

La cancelación de datos del trabajador tiene, en la normativa sobre protección de datos, una doble regulación. Por un lado, es un derecho que puede ejercer el trabajador ante el empresario[1035]al no estar interesado en que su información personal continúe en los ficheros de la empresa, hipótesis en la que el responsable del fichero tiene la obligación de informar al trabajador sobre el contenido, alcance y limitaciones de su derecho a la cancelación de los datos así como de la forma en la que podrá ejercerlo[1036]; y, por otra parte, la cancelación es una obligación impuesta al responsable del fichero –empresario- cuando los datos ya no son necesarios para el cumplimiento del objetivo que propició su recogida[1037] (en el supuesto de las relaciones de

[1033] Información disponible en http://www.eduardolagaron.com/wp-content/uploads/2011/02/proteccic3b3n-de-datos-en-el-c3a1mbito-laboral1.pdf;http://www.legaltoday.com/opinion/articulos-de-opinion/sistemas-de-whistleblowing-o-denuncias-anonimas-en-empresas-cuando-espana-navega-en-solitario [Consulta 5/09/2015].
[1034] Sobre la configuración de los derechos de acceso, rectificación, cancelación y oposición vid., el apartado 3.4. del Capítulo I.
[1035] Art. 16.5 de la LOPD: *"Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado".*
[1036]Vid., apartado 3.4. del Capítulo I.
[1037]En este sentido la OIT establece en sus Recomendaciones prácticas sobre el tratamiento de datos personales de los trabajadores (apartado 8.5) que : "*Los datos personales deberían guardarse únicamente durante un período que esté justificado por los fines concretos para los cuales hayan sido recabados, salvo que: a) un trabajador desee figurar en la lista de candidatos potenciales a un empleo por un período determinado; b) la legislación nacional disponga que los datos personales deban conservarse; o c) los empleadores o los trabajadores*

trabajo, el mantenimiento y gestión de la administración del personal de su empresa[1038]), sin que sea necesario que el trabajador titular del manifieste su deseo de excluir esa información de las bases de datos[1039].

Cuando es el propio trabajador el que solicita la cancelación de sus datos personales, ubicados en los ficheros de la empresa, se tiene que atender a lo previsto en el art. 16 de la LOPD[1040]. Este derecho se configura como un derecho personalísimo[1041] que sólo podrá ejercer el trabajador –persona física titular de los datos- , aunque también está previsto que en algunas ocasiones –incapacidad o minoría legal- un representante legal del afectado, debidamente acreditado, pueda invocar el derecho de cancelación en beneficio de su representado[1042].

Siguiendo los criterios que se han expresado de forma repetida, es obvio que, cuando finaliza el vínculo contractual[1043], se tiene que proceder a la cancelación de los datos sitos en los ficheros empresariales ya que han dejado de ser necesarios para cumplir con fines relacionados con el sostenimiento, gestión y control de la relación laboral, ahora terminada. El principal objetivo del

---

necesiten estos datos por razones legales para presentar pruebas sobre cualquier cuestión concerniente a una relación de empleo anterior o actual".

[1038] Art. 4.5 de la LOPD: *"Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos".*

[1039] FERNÁNDEZ VILLAZÓN, L.A.: "Tratamiento automatizado de datos…", op. cit., pp. 515-521. RODRÍGUEZ ESCANCIANO, S.:"La potencialidad lesiva de la informática sobre los derechos del trabajador" *Revista Española de Protección de Datos*, núm. 2, 2007, pp. 118-119.

[1040] Art. 16 de la LOPD:

[1041] Art. 23 del RDLOPD: "*Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado".*

[1042] Sobre la capacidad para ejercer el derecho de cancelación vid., Informe 409/2004 de la AEPD, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protegidos/common/pdfs/2004-0409_Acceso-por-el-titular-de-la-patria-potestad-a-las-historias-cl-ii-nicas-de-los-menores.pdf [Consulta 25/08/2015]. En el mismo, se diferencia entre menores de 14 años y mayores de esta edad valorando la capacidad del mayor de 14 años como suficiente para decidir sobre ellos mismos en el ámbito del derecho de cancelación, pudiendo ejercer este derecho salvo limitación legal expresa.

[1043] Sobre las distintas formas de extinción de la relación de trabajo véase: VV.AA.: *Extinción del contrato de trabajo*, Tirant lo Blanch, 2013.; VV.AA.: *Modalidades de extinción del contrato de trabajo: análisis de su régimen jurídico*, Comares, 2014.; MORALES VALLEZ, C.: *Extincion del contrato de trabajo : causas objetivas y disciplinarias, el fogasa*, Colex, 2014.

derecho de cancelación de los datos es evitar que los datos almacenados se vuelvan permanentes convirtiéndose en etiquetas definitivas para la persona –trabajador- con el peligro que esta situación puede provocar en su identidad y sus derechos. Esta situación podría agravarse en el ámbito de las relaciones de trabajo, si permanecen en la empresa referencias a situaciones pasadas y ya superadas que pudieran, en un determinado momento, impedirle acceder a un puesto de trabajo[1044].

A pesar de estar el derecho de cancelación regulado en el mismo precepto normativo que el derecho de rectificación, como se ha visto[1045], son dos derechos distintos[1046] que pueden llegar a complementarse pues, cuando un trabajador procede a rectificar los datos obrantes en el fichero de empresa, el empresario debe eliminar de la base de datos la información que ha sido modificada[1047]. Así pues, son también diferentes los momentos en los que se ejercen ambos derechos ya que la rectificación de datos del fichero empresarial se produce mientras el trabajador forma parte de la empresa; y en cambio, la cancelación se materializa una vez que se ha extinguido la relación de trabajo, puesto que no tiene sentido mantener esos datos si no se tiene que realizar ninguna gestión con la información de ese empleado por lo que, en estos casos, la modificación de los datos de los ficheros no suele darse porque estas informaciones ya han sido suprimidas[1048].

[1044] Sobre este aspecto vid., apartado 4.3 del presente Capítulo.
[1045] Vid., apartado 3.4. del Capítulo I.
[1046] Ya en el art. 31 del RDLOPD aparecen definidos de forma distinta: *"El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos. 2. El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento. En los supuestos en que el interesado invoque el ejercicio del derecho de cancelación para revocar el consentimiento previamente prestado, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente reglamento".*
[1047] Sobre este aspecto SERRANO PÉREZ, establece la presencia de dos derechos distintos, pues cada uno se dedica a una acción diferente. Así el derecho de rectificación corrige o actualiza un dato existente y el de cancelación lo que hace es permitir al titular del dato su eliminación del fichero, en SERRANO PÉREZ, M.: *El derecho fundamental a…*op.cit.pp.357-358; SALOM APARICIO, J.: *Estudio de la…,* op. cit., pp. 299-302.
[1048] La importancia de la actualización de las bases de datos alcanza un nivel elevado cuando se trata de bases de datos de personal, las cuáles pueden sufrir modificaciones como consecuencia de los cambios que pudieran darse a lo largo de la relación de trabajo no sólo en los datos identificativos del trabajador, sino también en aquellos relativos a las aptitudes profesionales del trabajador.

Sin embargo, en la normativa sobre protección de datos aparecen como dos derechos relacionados a la hora de fijar el procedimiento para ejercerlo. Como es sabido[1049], es en el art. 25 del RDLOPD en el que se regula el contenido de la solicitud para iniciar, no sólo el derecho de cancelación, sino para solicitar cualquiera de los derechos que la LOPD confiere a los titulares de datos de carácter personal. La solicitud del ejercicio del derecho de cancelación debe ser contestada en el plazo de diez días, independientemente si existen datos del interesado como si no hay constancia de ellos. Por tanto, si el empresario y responsable del fichero obstaculizará de forma sistemática el ejercicio del derecho incurriría en una infracción grave, regulada en el art. 44.4 e)[1050], hecho que conllevaría una sanción de entre40.001 a 300.000 euros[1051].

No obstante, hay situaciones en las que se pueden bloquear los datos en los ficheros empresariales con el objetivo de permitir su conservación para realizar, en lo que a las relaciones de trabajo se refiere, las gestiones laborales que el empresario tenga pendiente de resolver con ese trabajador que ya no forma parte de la empresa, informaciones relacionadas por ejemplo con la Seguridad Social, tributarias, de prevención, etc., o para atender los requerimientos de Jueces y Tribunales ante las denuncias interpuestas por el propio trabajador.

También se permite la conservación de los datos en los ficheros de la empresa si el trabajador así lo decide puesto que puede ser beneficioso para él seguir formando parte de esas bases de datos en vistas a futuras ofertas de empleo que puedan surgir en esa misma empresa[1052]. En estos casos, tanto el trabajador como el empresario pueden solicitar o realizar una cancelación parcial de los datos en aras a fomentar que se conserven sólo aquellos datos

[1049] Vid., apartado 3.4 del Capítulo I.
[1050] Art. 44.4 e) de la LOPD: "*El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición".*
[1051] Vid., art. 45.2 de la LOPD.
[1052] Como ya se ha visto en el Capítulo II en las ETTs es muy habitual que se mantengan los datos en los ficheros para posibles contrataciones que puedan darse y para las que sea necesario contar de nuevo con ese trabajador, a menos que el trabajador manifieste su intención de cancelar los datos a tenor de lo establecido en el art. 16 de la LOPD.

precisos para concurrir, por ejemplo, a otros procesos de selección que la empresa organice, y aquellos que sean útiles para el empresario ante posibles reclamaciones judiciales que le plantee el trabajador.

En la normativa laboral existen algunos plazos para la conservación de los datos de los trabajadores en los ficheros empresariales. Así, podrán permanecer en el fichero durante un año si se hubieran iniciado reclamaciones de cantidad ante los Juzgados y Tribunales del Orden Social, aunque ese plazo se puede incrementar si el conocimiento de la resolución judicial, por parte del empresario, no se produce de forma automática y pasa un tiempo desde que se dicta la sentencia hasta que ésta es conocida por el empresario[1053]. Cosa parecida ocurre con la obligación empresarial de conservar los registros o soportes informáticos relativos a altas, bajas, cotizaciones en Seguridad Social etc., así como la información relativa al IRPF del trabajador; supuestos en los que el período mínimo de conservación es de cuatro años, puesto que éste es el tiempo durante el cual la Administración puede exigirle algún tipo de responsabilidad al empresario[1054]. Por su parte, los recibos de salarios expedidos se archivarán y conservarán por las empresas, durante un período mínimo de cinco años[1055], a fin de permitir las comprobaciones oportunas.

[1053] Art. 5 de la Ley 25/2007: *"La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores".*

[1054] Art. 66 b) de la Ley 58/2003, de 17 de diciembre, General Tributaria (BOE núm. 302 de 18 de Diciembre de 2003): "Prescribirán a los cuatro años los siguientes derechos: *b) El derecho de la Administración para exigir el pago de las deudas tributarias liquidadas y autoliquidadas"*. Art. 52.1 del RD 84/1996: *"Los empresarios y, en su caso, los trabajadores por cuenta propia están obligados a conservar, por un período mínimo de cuatro años, los documentos justificativos de la inscripción del empresario, de la formalización de la cobertura y tarifación de las contingencias profesionales y de la cobertura de la prestación económica por incapacidad temporal, así como de la afiliación, altas, bajas y variaciones de datos de los trabajadores, en los términos regulados en el título anterior".*

[1055] Art. 3 de la Orden Ministerial, de 27 de diciembre de 1994, por la que se aprueba el modelo de recibo individual de salarios (BOE núm. 11 de 13 de enero de 1995): *"Los recibos de salarios expedidos se archivarán y conservarán por las empresas, junto con los boletines de cotización a la Seguridad Social, durante un período mínimo de cinco años, a fin de permitir las comprobaciones oportunas".*

Otro ejemplo de posible conservación de datos por parte del empresario es el relacionado con la formación bonificada que se haya impartido en la empresa. En este caso, las empresas deberán mantener a disposición de los órganos de control competentes la documentación justificativa de las acciones de formación comunicadas (tanto a efectos de bonificación como de cofinanciación privada) durante un periodo de cuatro años, contando a partir del momento en que haya finalizado el plazo de presentación de los documentos de cotización- del mes de diciembre de ejercicio en curso[1056]. En el supuesto de acciones cofinanciadas con fondos comunitarios (programa operativo 2007-2013)[1057], la documentación justificativa deberá estar a disposición de los órganos administrativos y de control, al menos, hasta el 31 de diciembre de 2020, según lo establecido por la normativa comunitaria[1058].

Una vez que termine el plazo de conservación establecido, los datos serán suprimidos de los ficheros de forma definitiva, es decir, se debe proceder a la cancelación por el procedimiento general establecido para ello. Sobre este tema cabe hacer una matización, sobre todo si se tiene en cuenta la posible petición en un futuro, por parte del trabajador, de un certificado en el que se expongan las tareas que ha realizado en esa empresa. Lo lógico es que este certificado se expida cuando ha finalizado la relación laboral, pero puede ocurrir que el trabajador lo solicite más adelante y que esos datos se hayan cancelado del fichero. Por este motivo, se debe mantener la cancelación parcial de los datos[1059], con el fin de que se pudieran conservar de forma indefinida tan sólo

[1056] Información disponible en http://www.fundaciontripartita.org/Con%C3%B3cenos/Pages/FAQ/PreguntasFrecuentesFormacionBonificadaRespuesta%20-20Procedimiento,%20requisitos% 20y%20obligaciones.aspx.[Consulta 22/03/2016].

[1057] Programa operativo Fondo Social Europeo (2007-2013). Adaptabilidad y empleo, disponible en http://www.empleo.gob.es/uafse_2000-2006/es/2007-2013/prog-operativos/Adaptabilidad-y-Empleo.pdf [Consulta 23/03/2016].

[1058] GONZÁLEZ BARTUREN, J.: "Bases de datos de recursos humanos…", op. cit., pp. 369-370; VV.AA.: "Reflexiones en torno a la protección de los datos de carácter personal", *Nuevas Políticas Públicas*. *Anuario para la modernización de las Administraciones Públicas*, Instituto Andaluz de Administración Pública, núm. 1, 2005, pág. 29; RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos…,* op. cit., pp. 158-160.

[1059] Sobre la cancelación parcial de datos y de forma análoga vid., Sentencia de la Audiencia Nacional de 26 de junio de 2012 (RJCA 2012\720): *"El legítimo ejercicio de su derecho resulta vulnerado cuando pese a ejercer el derecho de cancelación en relación con unos datos policiales concretos se subordina su eficacia a la utilización de un formulario concreto que tan solo permite cancelar los datos de un fichero policial concreto, pues no es exigible condicionar el ejercicio de este derecho a la utilización de dicho formulario ni limitarla a un fichero si la*

los datos relacionados con el desarrollo de la prestación de trabajo por parte del trabajador en la empresa.

Indudablemente, el responsable de cancelar los datos, atendiendo a la solicitud de cancelación del interesado -trabajador- o a la desaparición de la finalidad que propició su grabación y archivo en las bases de datos empresariales, es el empresario. Si, como puede ser habitual, la empresa contrata los servicios de una empresa externa para que administre los ficheros de datos de la empresa referidos, el responsable será el encargado de tratamiento. En estos casos, la base de datos no se encuentra ubicada en la empresa donde el trabajador ha prestado sus servicios, por lo que lo lógico será que el trabajador ejercite su derecho de cancelación ante este encargado del tratamiento[1060], siendo el empresario, que contrata al trabajador, el que les notifique esta circunstancia a sus empleados.

La figura del encargado del tratamiento está definida de forma más específica en el RDLOPD[1061], normativa que prevé también la cancelación de

---

petición reúne los requisitos sustantivos necesarios para acceder a la cancelación, sin que tampoco pueda obligarse al afectado a indagar cuales son los diferentes ficheros policiales en los que los que ha quedado reflejadas unas detenciones o hechos cuya cancelación se pretende, pues una vez identificados los antecedentes o datos que se pretenden cancelar y aportadas las Sentencias o resoluciones judiciales que justifican la procedencia de la cancelación solicitada, es la autoridad administrativa que ha introducido estos datos en diferentes ficheros la que ha de cancelar los datos que figuran en los mismos bien por sí misma bien comunicándolo a la autoridad responsable de los mismos haciéndole saber el derecho de cancelación solicitado"..

[1060] MARTÍNEZ FONS, D.:"Tratamiento y protección de datos de los trabajadores en la relación de trabajo" en VV.AA.: *Derecho Social y Nuevas Tecnologías*, CGPJ, 2005, pp. 68-70.

[1061] Art. 20 del RDLOPD: *"1. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente Capítulo. El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido. No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado. 2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este Capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento. 3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente. No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un*

datos ejercida ante él[1062]. En el ámbito laboral y más concretamente para la gestión de recursos humanos, el encargado del tratamiento se configura como un sujeto que colabora, desde su propia sede física, con la empresa en las tareas relacionadas con la administración de personal. Por lo que estos encargados serán entidades externas a la empresa con la que ésta mantiene una relación contractual a través de la cual la empresa externa se compromete a realizar todos los trámites relacionados con la contratación de los trabajadores y las vicisitudes que se puedan dar entorno a ese contrato de trabajo –pagos del salario, tramitación de alta y bajas por enfermedad, extinción del contrato de trabajo, etc.-[1063].

No obstante, a pesar de estar reconocida la facultad de cancelar los datos, al encargado del tratamiento puede ocurrir que finalmente se responsabilice de esta acción al empresario que contrata al trabajador, si previamente así se ha establecido en el contrato que éste ha firmado para la gestión de datos de sus empleados con una empresa externa. En este caso será el empresario, y no el encargado del tratamiento el responsable de recibir las solicitudes de los trabajadores cancelando sus datos y de responder a las mismas, según el procedimiento de cancelación establecido para ello[1064].

En cuanto a la conservación de los datos por el encargado de tratamiento tras la finalización del contrato de servicios suscrito entre tal encargado y la empresa dónde los trabajadores prestan sus servicios, el art. 22 del RDLOPD[1065] establece que no puede darse, ya que ha terminado relación

---

tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente Capítulo".

[1062] Art. 12.3 de la LOPD: "Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".

[1063] Si se configuran estas relaciones, la empresa que colabora en la gestión de recursos humanos será también la encargada de realizar las comunicaciones de datos pertinentes a las administraciones públicas, respetando los principios de la LOPD previstos para estas cesiones (vid., apartado 5.1.del Capítulo III).

[1064] Vid., Informe jurídico 472/2008 de la AEPD, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2008-0472_Encargado-de-tratamiento-de-datos-sensibles-de-fichero-p-uu-blico.-Derecho-de-cancelaci-oo-n.pdf [Consulta 22/12/2015].

[1065] Art. 22 del RDLOPD: *"Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que*

contractual entre ambas empresas, por lo que no existe ningún objetivo que justifique el mantenimiento de los datos en los ficheros de la empresa encargada de la administración de la información personal de sus empleados. Así pues, los datos de los trabajadores deben retornar a los ficheros del responsable, si éste estuviera obligado a conservarla durante un tiempo determinado. Al margen de esta obligación también pesará sobre el responsable del fichero la de destruir, eliminar o cancelar los datos, que, vinculados al contrato de servicios, no deban mantenerse; y también la de atender, si lo estima pertinente, las solicitudes de cancelación de datos presentada por los trabajadores afectados.

Como última hipótesis, puede ocurrir que, además de los ficheros conocidos por el propio trabajador, existan en la empresa otras bases de datos complementarias , pero ocultas y llamadas por eso listas negras, en las que se incluya información variada acerca del comportamiento del trabajador en la empresa y de cualquiera de las facetas de desarrollo de su actividad y de su relación con la empresa. Como es lógico, estos datos se consideran de carácter personal porque son informaciones que van unidas a aspectos que identifican a una persona, por ejemplo, el registro de informaciones acerca de ciertos incumplimientos del trabajador en la realización de la tarea encomendada, determinados tipos de comportamientos, incidentes, actitudes, valoraciones, etc.

En lo que aquí interesa, habrá que delimitar, en primer lugar, la legalidad de esos ficheros que han sido configurados sin la conformidad de los titulares de esos datos –en este caso trabajadores-. Por lo que, en un principio, se puede afirmar que la constitución de las bases de datos de trabajadores, no cumple con las exigencias marcadas por la LOPD a menos que el empresario justifique esta actuación en la excepción al consentimiento para el tratamiento

---

éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación. 2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento".

de datos establecida en el art. 6.2 de la LOPD, basada en el procesamiento de información sin consentimiento para el mantenimiento de la relación de trabajo, lo cual no tiene sentido si ese fichero se conserva una vez extinguido el contrato laboral.

Al margen de la legalidad y constitucionalidad del almacenamiento de este tipo de información, el uso empresarial que se pueda hacer de este tipo de información (tanto la propia empresa como otras del sector o vinculadas contractual o societariamente con la empresa de origen) suele tener efectos normalmente negativos para los trabajadores. Sucede que lo que se acumula es sobre todo datos de carácter negativo (obviamente desde la perspectiva de la empresa y en términos exclusivamente productivos, organizativos o económicos), la existencia de esa información y su tratamiento permite detectar a los trabajadores que, de nuevo desde la perspectiva de la empresa, no es aconsejable contratar. La relación de esos nombres, a los que se pretende condenar a lo que incluso en términos forenses se ha calificado como de "muerte profesional" es lo que constituye la "lista", que es negra en virtud de ese repudio general a su contratación[1066].

El problema se plantea cuando como consecuencia del mantenimiento de esos ficheros y de la falta de cumplimiento de la obligación de eliminar esos datos se perjudica al trabajador en su búsqueda de empleo, realizando el empresario un tratamiento de esa información. Recientemente el Tribunal Supremo[1067] ha condenado a una empresa por la cesión de datos de un

[1066] Concepto acuñado en el Documento de trabajo del Grupo del art. 29 sobre listas negras, de 3 de octubre de 2002, disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp65_es.pdf [Consulta 23/12/2015], como: *"Interferencias en la esfera individual de las personas que se generan por la incorporación de las mismas a bases de datos en las que se aparece identificado en relación con una situación o hechos determinados"*.

[1067] Sentencia del TS de 12 de noviembre de 2015 (RJ 2015\5063); *"En el presente caso, puede considerarse que el demandante había aportado al proceso indicios de que una conducta lesiva para sus derechos fundamentales podía haberse producido, en concreto, la cesión por parte de Cotronic de los datos personales del demandante asociados con una conducta lesiva para su honor (haber incurrido en una conducta contraria a la buena fe contractual por haber intentado cobrar a un cliente por una actuación por la que no tenía derecho a realizar tal cobro). Tales indicios son la declaración del miembro del comité de empresa de Telefónica que afirmó su convicción sobre la existencia de un fichero de trabajadores conflictivos formado no solo con los datos de Telefónica, sino también con las comunicaciones de empresas subcontratistas; el hecho de que el demandante, tras ser*

trabajador a otro centro de trabajo en el que éste pretendía prestar sus servicios, teniendo como resultado su no contratación[1068]. Esta comunicación de datos no cumple con lo establecido en el art. 11.3 c) de la LOPD, que no requiere el consentimiento expreso del afectado *"Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique"*, y de ahí que fuera válida la transmisión de los datos estrictamente relativos a la relación laboral como "nombre, apellidos, fecha de alta y baja en la empresa, y una fotografía", pero no lo sería en modo alguno, y vulneraría claramente la normativa protectora de datos personales aquella información que se refiriera al carácter conflictivo del trabajador, porque ello habría posibilitado la inclusión en "un fichero de trabajadores conflictivos" (obviamente, añado yo ahora, ajeno por completo y contrario a la normativa constitucional y legal), que impediría su contratación por empresas (contratas y subcontratas) que presten sus servicios para Telefónica. Finalmente, la Sentencia establece una indemnización para el trabajador por la infracción de su derecho a la protección de datos[1069], lo que a su vez le ha provocado un prejuicio materializado en la búsqueda infructuosa de empleo durante meses lo que ha sido directamente impedido por la información empresarial suministrada y tratada.

---

despedido de Cotronic, llevaba varios meses sin encontrar empleo; y el hecho de que tras pasar la entrevista de trabajo y ser sometido incluso a reconocimiento médico, no fuera finalmente contratado por Itete, sin que el director de recursos humanos de esta empresa, al declarar en el juicio, supiera precisar por qué no se le había contratado".

[1068] Documento de UGT http://www.smcugt.org/archivos/elementos/2015/informe_sts_lista negra. pdf. [Consulta 27/12/2015].

[1069] La indemnización queda fijada en los arts. 45.2 de la LOPD: "*Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros",* al considerarse, este hecho, una infracción grave del derecho a la protección de datos tal y como establece el art. 44.3 b) y c).

CONCLUSIONES

"Estudia las frases que parecen ciertas y ponlas en duda".
Riesman, David.

I. ASPECTOS GENERALES DE LA PROTECCIÓN DE DATOS Y SU AFECTACIÓN A LAS RELACIONES DE TRABAJO.

1. El derecho a la protección de datos de carácter personal ha ido adquiriendo cierta autonomía respecto al derecho a la intimidad, desde que en sede jurisprudencial (Sentencias 290/2000 y 292/2000 del TC) se reconoció su eficacia e independencia. No obstante, a pesar de esta distinción, en el terreno laboral, existen momentos en los que no se aprecia esa diferenciación desapareciendo individualidad para ser concebido como un derecho que se complementa con la intimidad de los trabajadores y que siguen teniendo mucha relación a la hora de producirse alguna vulneración.

2. Tras este estudio se puede concluir que la LOPD, reguladora del derecho a la protección de datos, se muestra como una norma desorganizada sistemáticamente al incluir, por ejemplo, dentro del Título II, en el que describen los principios para el tratamiento de datos de carácter personal, la noción de dato especialmente protegido así como la forma de proceder a la hora de comunicar y acceder a datos por parte de terceras personas. De otra parte, la rigidez de la normativa sobre protección de datos, en principios y conceptos, hace muy difícil su aplicación. Quizás, lo que pretende la norma es crear un paraguas de protección demasiado amplio pero, a su vez, no es consciente de la realidad y de la necesidad de tratar la información personal para realizar numerosas gestiones que son imprescindibles en el panorama laboral y administrativo, las cuáles hacen complicado respetar lo establecido en la legislación. A su vez, la normativa sobre protección de datos se presenta como una norma represiva, prohibiendo prácticamente todos los usos sin tener ninguna capacidad preventiva que pueda evitar un mal uso de los datos de carácter personal siendo, una norma de difícil aplicación a sectores muy concretos, en lo que aquí interesa a las relaciones entre empresario y trabajador.

3. Analizando la legislación actual sobre protección de datos y para poder comprender cuando se produce la vulneración de este derecho, es necesario conocer lo que la normativa entiende por tratamiento de datos, puesto que si no se dan ninguno de los criterios establecidos en la norma para su existencia no se estaría hablando de una lesión del derecho a la protección de datos, aunque si pudiera tratarse de una vulneración del derecho a la intimidad. Sobre este aspecto, la norma no parece demasiado precisa pues en el RDLOPD, en el que se clarifican y completan las definiciones dadas por la legislación sobre protección de datos, se admite dentro del concepto de tratamiento la consulta de los datos al igual que ocurre en la Directiva 95/16/CE pero, la LOPD no tiene en cuenta estas situaciones a la hora de concretar las actuaciones que pueden constituir un tratamiento de datos. También en la Directiva 95/46/CE se tiene en cuenta la consulta Por lo que, se produce una contradicción teniendo en cuenta que un simple acceso no constituye, a mi modo de entender, el sentido del procesamiento de datos y la aplicación de los principios que se describen en la LOPD, los cuáles se aplican para respetar aquellas informaciones que se recogen en un fichero, informatizado o no, que responda a una concreta estructura.

4. Se ha de entender que lógicamente el trabajador también es sujeto del derecho a la protección de datos, porque efectivamente intercambia información personal con el empresario que lo va contratar o que va a colaborar en su búsqueda de empleo. Sin embargo, no parece existir en el en el ámbito empresarial una cierta conciencia del alcance o perjuicio que se puede provocar al empleado cuando se trata su información personal de forma negligente, es decir, incumpliendo la normativa sobre protección de datos.

5. Teniendo en cuenta el más que evidente tratamiento empresarial de los datos de los trabajadores, la ausencia de legislación específica que desarrolle y regule el derecho a la protección de datos de éstos ha supuesto el estudio de esta disciplina desde distintas fuentes y opiniones que no alcanzan el vigor que pudiera otorgarle un respaldo normativo concreto. Este hecho llega a provocar cierta inseguridad jurídica, teniendo que aplicar para los conflictos que se puedan dar en el entramado de las relaciones de trabajo una norma

general, unido a la falta de precisión que la doctrina jurisprudencial aporta a la hora de resolver estos conflictos. Por ello, se hace necesario una legislación específica que regule no sólo la aplicación de los principios a los supuestos concretos que puedan manifestarse en las relaciones de trabajo, sino la forma de ejercer los derechos que la LOPD otorga a los ciudadanos más adaptada a la relación ciudadano-empresario. Esta necesidad se traduce en la posición que tiene el empresario como responsable del fichero, la cual puede suponer una amenaza que impida que el trabajador ejerza sus derechos por miedo a perder su puesto de empleo, ya que la perspectiva y el sentido del ejercicio de los derecho se puede perder si la persona ante la que tienes que desplegarlos ostenta la posición de" jefe" o intermediario en la búsqueda de empleo de ese desempleado.

6. En relación a la ausencia de protección de los datos de personas jurídicas se puede decir que, en este punto y en lo que a las relaciones de trabajo se refiere, esta desprotección permite a los trabajadores la cesión de datos privados de la empresa a terceros, sin que este hecho sea castigado por una supuesta infracción de la legislación sobre protección de datos. Si así ocurriera, estos empleados podrían incurrir en un ilícito relacionado con la competencia desleal, por filtrar información confidencial de la empresa, o por un incumplimiento de la buena fe contractual pero no podrían ser castigados por vulnerar el derecho a la protección de datos, puesto que la entidad empresarial no forma parte del ámbito subjetivo de este derecho.

7. Otro aspecto destacable, y que también puede influir en el ámbito laboral, es la distinción entre ficheros públicos y privados mantenida por la LOPD. Parece extraño que se mantenga esa diferenciación cuando la Directiva 95/46/CE no la contempla y que sólo se justifica desde la situación de privilegio que han alcanzado las Administraciones públicas en el ámbito de la protección de datos. Si se traslada esa catalogación de los ficheros al ámbito laboral se puede decir que su funcionalidad carece de sentido, ya que la mayoría de datos que maneja el empresario son trasladados a la Administración para la formalización del contrato de trabajo o para poder realizar trámites relacionados con la administración del personal de su empresa, pasando a formar parte de

ficheros públicos y estando gestionados por entidades públicas, a las que se le exigen menos requisitos para la configuración de las bases de datos e, incluso, para las pertinentes cesiones que se produzcan entre ellas. Por este motivo, tendría que regularse un solo tipo de ficheros para no perder la esencia de lo que realmente se protege que es la información personal de los ciudadanos, sin que la titularidad del fichero pudiera provocar una situación más beneficiosa a la hora de tratar esos datos.

8. Sobre la obligatoriedad en la inscripción de ficheros hay que matizar que hasta la entrada en vigor de la LOPD no se tenían que registrar los ficheros manuales, por lo que aquellos creados antes de la promulgación de nuestra normativa actual de protección de datos estaban exentos del registro ante la AEPD. Ante esta realidad y teniendo en cuenta la cantidad de datos de trabajadores que se archivaban en las empresas de forma manual, la falta de alguna disposición normativa que regulara este aspecto ha provocado que muchas de esas informaciones se pierdan y no se tenga constancia de si realmente cumplían con las exigencias marcadas en esa época, por la ya derogada LORTAD.

9. Ahora bien, sobre el consentimiento para tratar los datos de los ciudadanos se observa como la norma, en realidad al ser una ley que regula aspectos generales, no ofrece garantías al trabajador. De ahí que se produzca una cierta privación en la libertad de decisión del trabajador para consentir el tratamiento de datos que le pide el empresario, vinculada al interés que tiene ese empleado por conseguir o conservar el empleo. Si ese consentimiento se presta por las presiones ejercidas por el empresario no se debe considerar válido, ya que no se cumple con la libertad para decidir instaurada en la definición de consentimiento dada en la LOPD.

10. Como es sabido, la LOPD establece una excepción al consentimiento que es totalmente aplicable al ámbito de las relaciones de trabajo, referida al tratamiento de datos que puede realizar el empresario sin la conformidad del trabajador basándose, para ello, en que ese procesamiento de datos es necesario para el mantenimiento del contrato de trabajo. Por este

motivo, esta excepción aplicada a la gestión de datos en el centro de trabajo requiere alguna que otra matización, ya que de lo contrario el empresario puede efectuar muchos tratamientos de datos sin que medie la conformidad del trabajador, fundamentando esta actuación en el sostenimiento de esa relación contractual, sin tener en cuenta que con ese procesamiento de datos pudiera perseguir otros objetivos incurriendo, entonces, en una infracción del principio de calidad pero no del de consentimiento.

11. La catalogación del consentimiento para tratar los datos personales como inequívoco, no deja lugar a equivocación, plantea un problema y es el relacionado con la posibilidad de acreditar que efectivamente se ha prestado. En el panorama empresarial este hecho se puede solventar con la firma de un anexo al contrato de trabajo en el que quede constancia que el trabajador ha consentido el tratamiento de los datos, creando una prueba documental que genera cierta seguridad en la utilización de la información personal que realice el empresario, puesto que tiene un documento que lo habilita para tratar los datos de sus empleados. De esta forma, quedará acreditada la prestación del consentimiento pero, no se soluciona el clima de presión indirecta existente, entre empresario y trabajador, generado para que el empleado firme el documento.

12. En cualquier caso sobre la forma de prestar el consentimiento para tratar datos especialmente protegidos, no tiene sentido que para los datos relacionados con la salud se exija consentimiento expreso y para las informaciones acerca de la afiliación sindical éste tenga que ser expreso y además otorgarse por escrito. El legislador tendría que haber uniformizado la forma de solicitar el consentimiento en los dos tipos de datos, ya que puede resultar igual de atentatorio, o más si cabe, el tratamiento de datos sobre la salud de los trabajadores.

13. Un ejemplo más de la problemática presenta la aplicación de una ley general a un sector específico, como es la regulación de las relaciones de trabajo, lo constituye la responsabilidad del fichero. En este punto, se puede observar como la responsabilidad del fichero la tiene el empresario pero, en

ocasiones, no es la persona encargada de tratar los datos de los trabajadores porque estas actuaciones la realizan los propios empleados. Por esta razón, y para velar por la información personal que discurre en las distintas estancias empresariales, sería conveniente que el empresario incentivara la utilización de esos datos conforme a la normativa sobre protección de datos, facilitando a sus trabajadores prácticas formativas en esta disciplina, sobre todo de aquellos que realicen tareas relacionadas con la gestión del personal de su empresa.

14. Ante esta realidad y teniendo en cuenta que son los propios trabajadores los que tratan información de sus compañeros de trabajo, no queda del todo claro la responsabilidad que se le puede exigir. No se puede decir que estos trabajadores ostenten la figura de encargado del tratamiento, ya que en su contrato de trabajo quedan establecidas sus funciones generales, sin contener, como regla general, advertencias acerca de la posible responsabilidad que tendrían si hacen una utilización de los datos poco diligente. Para poder exigirle algún tipo de obligación respecto al tratamiento de datos, con los criterios establecidos en la normativa, es necesario que mediara un contrato de hospedaje entre ese empresario y los trabajadores que procesan los datos de carácter personal, por lo que si éste no existe la responsabilidad acerca del uso de ese fichero de datos la tiene únicamente el empresario.

15. Con lo expuesto y ante publicación del Reglamento General de protección de Datos, días antes de la finalización del presente trabajo, se hacen necesarias las siguientes reflexiones, ya que se tratan aspectos de forma más concreta que podrían al desarollo del derecho a la protección de datos en el ámbito laboral.

a. Dentro del apartado dedicado a las definiciones (art. 4) se alude al término elaboración de perfiles referido a “toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad,

comportamiento, ubicación o movimientos de dicha persona física". La inclusión de este concepto está vinculada al tratamiento de datos realizado por los intermediadores laborales, encontrado en el RGPD un acercamiento a este tipo de actuaciones encaminadas a la consecución del candidato al empleo más apropiado.

b. Acerca de la instauración de un Delegado de Protección de datos en empresas, se puede decir que esta figura será necesaria en la mayoría de centros de trabajo que utilicen los sistemas de monitorización sistemática de los trabajadores, debido a la gran escala de datos que van a llegar a manejar. Aunque, también se debe implantar esta figura en aquellas empresas que traten datos que revelen el origen racial o étnico, ideología, religión o creencias filosóficas, afiliación sindical, datos genéticos, y el tratamiento de datos biométricos para identificar unívocamente a una persona, así como los relativos a la salud y vida y orientación sexual, y datos relativos a condenas y antecedentes penales.

c. Considera inválido el consentimiento prestado, cuando éste se otorgue mediando un desequilibrio claro entre el interesado y el responsable del tratamiento. Este criterio, es esencial y perfectamente aplicable a las relaciones de trabajo para evitar que la situación de dependencia del trabajador respecto al empresario no genere la obligación por su parte de tener que dar conformidad al tratamiento de sus datos de carácter personal. Si así se hiciera perdería sentido la excepción al consentimiento para mantener una relación contractual, ya que en todas ellas existe una parte que tiene una posición jerárquica inferior a la otra.

d. El RGPD prevé que la AEPD tenga muchas más funciones de control, pues establece que apruebe los Códigos de Conducta de la empresa y que estos sean también publicados; que realice un listado con aquellos tratamientos de datos que requieran un estudio de impacto debido al riesgo que supone para los derechos de las personas físicas; que reciban de los responsables de los ficheros, en el plazo de 72 horas, las posibles violaciones

de seguridad sobre la información protegida, etc.

e. Por último, el RGPD contempla e insta a los distintos Estados Miembros a que a través de disposiciones legislativas o de convenios colectivos, establezcan normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

II. ASPECTOS RELACIONADOS CON LA INTERMEDIACIÓN LABORAL, LA RELACIÓN DE TRABAJO, Y LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

16. La innovación tecnológica también ha hecho incursión en la intermediación laboral presentándose como un medio que permite al desempleado la facultad de acceder a un mayor número de ofertas de empleo con la simple visita a las webs de estas empresas, y por otra parte posibilita al intermediador el registro y filtrado de todas las candidaturas que se reciben a través de la web. No obstante, la proliferación de esta forma de intermediación deja fuera a un sector de la población sobre todo a aquellos desempleados de edad más avanzada que no están familiarizados con las TICS y a los que no tienen acceso a internet o no tienen la suficiente formación como para poder navegar por la web. Por este motivo, se debería continuar recogiendo en las empresas dedicadas a la selección de personal los CV en formato papel para procurar un servicio que llegara a todas las personas que estén buscando trabajo, al igual que también se tendrían que publicar en prensa o en anuncios de empleo más ofertas de las que actualmente se anuncian.

17. Estos portales de empleo, pertenecientes a entidades públicas o privadas, deben cumplir con la normativa sobre protección de datos, pues a través de ellas se recoge información personal que es almacenada en ficheros. Por ello, deben contener un sitio en su web dónde se le informe debidamente del sentido y finalidad que tiene esa recepción de información y cuál va a ser el tratamiento de datos que se va a realizar. Del análisis de las distintas páginas webs se puede concluir que, las advertencias sobre el tratamiento de datos dadas en los portales de empleo gestionados por empresas de intermediación pública es más escasa. que las proporcionadas en las de naturaleza privada. No se entiende porqué en estos portales webs no se llega a transmitir una información más detallada sobre el procesamiento de datos de los demandantes de empleo, independientemente de que las personas que se encarguen de tratar esa información conozcan la normativa y las exigencias relativas al tratamiento de datos y de que el acceso sea más restringido al estar mejor estructurada las funciones de cada empleado público.

18. La internacionalización de los datos de los demandantes de empleo, propiciada por el uso delas TICs, se convierte en un medio capaz de universalizar tanto ofertas como demandas de empleo, ya que permiten que nuestra sociedad llegue a estar fusionada tecnológicamente. Por este motivo, el Derecho tiene que aportar respuestas a esta nueva realidad y actuar en consecuencia para que se proteja la información de los trabajadores que se transmiten fuera de nuestras fronteras, teniendo en cuenta que lo peligroso no es el simple movimiento de esa información, sino la ausencia de reconocimiento del almacenamiento internacional de esos datos que tiene lugar con esa cesión, creando un nuevo fichero en aquellos países en los que se destina la información.

19. La protección sobre la internacionalización de los datos ha sufrido recientemente un retroceso al ser derogada por el TJUE la Decisión 2000/520/CE de la Comisión Europea, la cual cubría la ausencia de tutela de los datos cuando se hacían transferencias a países que no disfrutaban de un nivel de protección equiparable a la LOPD. La supresión de la citada Decisión

tiene efecto en el panorama de la intermediación laboral, ya que la información inserta en las redes sociales profesionales, utilizadas como medio para buscar demandantes de empleo, están exentas de protección si el proveedor de la red social no pertenece a alguno de los países que gozan del nivel adecuado de protección. Por este motivo, todas aquellas redes sociales que tienen su origen en EEUU (país que a raíz de la anulación de la Decisión no ostenta un nivel de protección equiparado a la LOPD) no pudiendo, en estos casos, alegar incumplimiento de la normativa española sobre protección de datos, aspecto que debe ser advertido en la política de privacidad de las propias redes sociales generales y profesionales.

20. En esta línea y como mecanismo de averiguación de más datos de los usuarios de las redes sociales existe un servicio premium para acceder a un mayor número de perfiles, el cual puede interesarle a los agentes de intermediación que usen las redes sociales como medio para buscar, organizar, y comunicarse con potenciales candidatos. Los suscriptores de este servicio de pago pueden exportar cierta información de los perfiles de los miembros de la red social, para gestionar eficazmente la información de los candidatos, por lo que se está “vendiendo” información y, por lo tanto, negociando, con los datos identificativos y profesionales de los usuarios en ellas inscritos. Sobre este asunto, se puede decir que no se entiende como una red social gratuita puede tarificar determinados servicios y permitir que con el correspondiente pago se pueda acceder a más datos de los usuarios.

21. Para intentar paliar estos problemas, las empresas de intermediación deben establecer unas pautas sobre el uso de las redes sociales y orientar a los empleados sobre lo que es aceptable o no a la hora de utilizarlas como medio de reclutamiento de personal. Estos códigos de conducta deben respetar la normativa sobre protección de datos de carácter personal y los citados dictámenes específicos sobre el tema. Al igual que, sería interesante que la empresa comunicará o informara en su web corporativa cuáles son las redes sociales con las que trabaja, para que de esta forma el candidato supiera que las consultan a la hora de realizar un proceso de selección de personal.

22. La regulación del derecho al olvido en internet a través de una norma que estableciera las distintas exigencias para el mantenimiento de datos en los buscadores webs, lograría que aquellas informaciones relacionadas con aspectos que no cumplan con la finalidad del motor de búsqueda no fueran determinantes, por ejemplo, para catalogar a una concreta persona física de un modo que pudiera perjudicar su posible acceso a un puesto de trabajo. Lógicamente, los seleccionadores que utilizan esta técnica de búsqueda de información personal de los candidatos de empleo tampoco cumplen, realizando esa acción, con el objetivo de encontrar el trabajador con más capacidad para el trabajo que demandan, pues la averiguación de la aptitud debiera devenir por los distintos métodos reseñados en este trabajo. En ocasiones, el empresario también hace uso de estos medios para averiguar datos acerca de sus trabajadores que nada tengan que ver con su diligencia a la hora de efectuar su prestación de trabajo incumpliendo, también, con la finalidad en el tratamiento de esa información.

23. En lo que respecta al secreto profesional, sobre los datos médicos de los trabajadores, evidentemente éste debe mantenerse y únicamente debe transmitirse a la empresa aquella información necesaria para acreditar o no la capacidad de los empleados a la hora de ejercer un determinado puesto de trabajo. Ahora bien, estos trabajadores podrían tener algunas deficiencias psicológicas que pudieran ser conocidas o diagnosticadas por otros profesionales médicos distintos de los que realizan los reconocimientos médicos de empresa. En estos casos debe plantearse, y teniendo en cuenta las funciones que éstos trabajadores realizan, si no debiera de existir una conexión entre estos médicos y el empresario para que pudieran éstos profesionales sanitarios, ajenos al desarrollo de los controles médicos empresariales, certificar la ausencia de aptitud del empleado a la hora de desarrollar esa actividad en un determinado momento.

24. Debido a la gran cantidad de cesiones de datos que realizan las empresas de intermediación, la AEPD podría instalar un registro en el que los candidatos supieran a que empresas han ido a parar sus datos y tuvieran la opción de cancelar los datos online, no solo de la empresa de intermediación

en concreto sino de todas aquellas que hubieran tenido conocimiento de su información personal.

25. Esta solidaridad empresarial, relativa a las conclusiones vertidas por un empresario sobre los trabajadores que han trabajado en su empresa, no se podría llevar a cabo si se hubieran cancelado los datos de los ficheros de recursos humanos de la empresa. Lo lógico sería cancelar la información de aquellos trabajadores que por una u otra razón ya no forman parte de la plantilla de la empresa, sobre todo aquellos relacionados con la producción del trabajador en la empresa que, realmente, debieran ser los que pueden interesar a otro empresario a la hora de contratar a un trabajador. No obstante, el empresario podría dar otros datos que nada tienen que ver con la actividad productiva del trabajador y sobre esos no existe control, puesto que son opiniones referidas al comportamiento y la actitud del trabajador en la empresa, las cuales deberían de ser tratadas de forma menos objetiva que aquellas relativas a la capacidad productiva del trabajador.

III. ASPECTOS RELACIONADOS CON LAS TICS Y EL DERECHO A LA PROTECCIÓN DE DATOS DE LOS TRABAJADORES.

26. En un mundo y concretamente en una sociedad laboral cada vez más estigmatizada por la incursión de las TICS, no tiene sentido la falta de regulación de la problemática que estos medios pueden ocasionar al desarrollo del derecho a la protección de datos del trabajador. Por ello es necesario, además del establecimiento de exigencias específicas para la preservación de la información personal de los trabajadores, desde que las nuevas tecnologías han hecho su incursión en la empresa, también la implantación de instrucciones que dirijan los límites en el uso personal de la informática. A su vez, es preciso aclarar y completar las definiciones de la LOPD para poder adaptarlas a los requerimientos que conlleva la informatización de los medios de trabajo, sobre todo precisando el concepto de fichero automatizado, tratamiento automatizado y otras definiciones conexas a la hora de crear bases de datos con información privada de los trabajadores de la empresa.

27. No obstante, el empresario puede establecer mecanismos, gracias a la tecnología moderna, para bloquear el acceso a través de Internet a sitios no autorizados o el filtro de correos electrónicos recibidos por los empleados. Si así se hiciera se podría evitar que este empleador conociera información personal de los trabajadores, ya que la adopción de estas características técnicas permiten el debilitamiento de la propia necesidad de llevar a cabo controles que puedan ser reveladores de otros datos personales que no tengan relación con la supervisión de la prestación de trabajo de esos empleados. En la serie de operaciones de control, llevados a cabo por el empleador, que puedan considerarse incompatibles con la protección de la confidencialidad y la privacidad es parte del interesante caso de la utilización de equipos destinados a tomar las huellas dactilares, CD sensor biométrico, u otros sistemas similares, pues lógicamente con su instalación no sólo se conocen indicaciones acerca del cumplimiento de la jornada laboral , sino que la propia configuración de estos instrumentos desvelan datos sensibles del trabajador.

28. En cualquier caso, la instalación de medios de control de acceso debieran restringirse o limitarse a aquellos mecanismos que tan sólo dieran información relacionada con la hora de entrada y salida al centro de trabajo. La peligrosidad que presenta la averiguación de otros datos superfluos o complementarios a los realmente precisos para controlar la prestación de trabajo, como pueden ser la revelación de datos relacionados con la salud de los trabajadores, hace que estos mecanismos sean demasiado intrusivos con el derecho a la protección de datos de carácter personal.

29. En este sentido, tampoco la normativa sobre protección de datos aporta soluciones a los problemas que puede generar el avance de los medios tecnológicos en la empresa como consecuencia del procesamiento de datos que realizan. Prueba de ello, es la velocidad con la que se actualizan los medios tecnológicas y la falta de respuesta que la ley puede aportar ante estos cambios, debido a la dificultad de crear normas en un plazo de tiempo tan breve que se adapten a las necesidades que presenta la actual sociedad de la información.

30. Existe, actualmente, una preocupación por controlar al trabajador a través de las TICS que quizás estén descuidando otros aspectos en la empresa. Puede que las TICS en vez de colaborar en la realización de las tareas administrativas de forma más ágil y eficaz supongan, para el trabajador, una forma de control desmesurada, ya que es una manera realmente sencilla de comprobar la falta de actividad del trabajador, sin tener en cuenta que si no existieran también se perdería el tiempo de igual forma, por ejemplo, mirando a través de la ventana del despacho o manteniendo conversaciones con otros compañeros, y la supervisión de estas conductas tiene un menor seguimiento por parte del empresario.

31. La problemática que plantea el uso del correo electrónico o de internet por parte de los trabajadores durante su jornada laboral se vería minorada si el empresario estableciera unas instrucciones sobre la utilización de esos medios, siendo estos códigos de conducta aceptados de forma positiva por el trabajador, limitándose a utilizarlos de la manera sugerida por el empresario. Como de la práctica de estos controles se tratan datos de carácter personal, el trabajador debe conocer el destino y uso de su información personal y consentir este hecho para que el empresario no vulnere el derecho a su protección de datos de carácter personal.

32. Sin embargo, existen situaciones en las que el establecimiento de algunos sistemas de control pueden beneficiar al trabajador. Como se ha comentado, la obligación de instalar un sistema electrónico del control horario del trabajador se presenta como una medida ventajosa para poder tener en cuenta las horas extras que se realicen en la empresa y, por tanto, los derechos retributivos que le corresponden a cada empleado por este reconocimiento.

ANEXOS

BIBLIOGRAFÍA.

ABERASTURI GORRIÑO, U.: "Movimiento Internacional de Datos. Especial referencia a las transferencia internacional de datos sanitarios" *Revista de Administración Pública,* núm. 186, 2011.

ABJORSSON, B.: "Relación entre la protección de datos y la libertad de prensa y de expresión" en TRONCOSO REIGADA, A, (dir): *Transparencia administrativa y protección de datos personales*, Civitas, 2008, pp. 304-305.

ADSUAR Y.: "Cloud computing vs protección de datos de carácter personal" *Actualidad Jurídica de Aranzadi*, núm. 846, 2012.

AGENCIA DE DERECHOS FUNDAMENTALES DE LA UE*: Manual de legislación europea en materia de protección de datos,* 2014, pp. 187-188, disponible en: http://www.echr.coe.int/Documents /Handbook_data_protection_SPA.pdf*.*

AGUILERA IZQUIERDO, R.: "*El ejercicio de las facultades de vigilancia y control por el empresario a través de agencias de detectives,* Revista Española de Derecho del Trabajo, núm. 158, 2013.

AIMO, M.P.: "Tutella della riservatezza e protezione dei dati personali dei lavoratori" en VV.AA.: *Tratato di diritto del lavoro*, vol. IV, tomo II, Padova, CEDAM, 2012.

ALARCÓN CARACUEL, M. R.: "La informatización y las nuevas formas de trabajo" en VV.AA. *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Bomarzo, Albacete, 2004.

ALASTRUEY, R.: *Empleo 2.0*. Editorial UOC, 2009.

ALGAR JIMENEZ, C.: "España: La Protección de Datos de los Trabajadores y su Tratamiento por la Representación Sindical" *AR. Revista de Derecho Informático,* núm. 94, 2006.

ALGUACIL GONZÁLEZ-AURIOLES, J.A.: "La libertad informática: aspectos sustantivos y competenciales (SSTC 290 y 292/2000)", *UNED: Teoría y Realidad Constitucional*, núm.7, 2001.

ALMUZARA ALMAIDA, C. (coord.) *Estudio práctico sobre la protección de datos de carácter personal*, Lex Nova, 2005.

ALONSO VEGA, M.T.: "La RED EURES: libre circulación de trabajadores y empleo en la UE", *Boletín asturiano sobre la Unión Europea,* núm. 82-83, 1999.

ALUJAS RUIZ, J.A.: "La eficacia del servicio público de empleo en España. Análisis de la intermediación laboral a nivel autonómico", *Tribuna de Economía*, núm. 841, 2008.

ALUJAS RUIZ, J.A; "El servicio público de empleo y su labor como intermediario en el mercado de trabajo en España", *Cuadernos de Ciencias Económicas y Empresariales*, núm. 53, 2007.

ÁLVAREZ ALONSO, D.: "Modulación laboral de los derechos fundamentales, ponderación y principio de proporcionalidad. ¿Un paradigma en retroceso?", *Comunicación presentada al XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social*, Pamplona, 2014.

ÁLVAREZ CIENFUEGOS, J.M.: "La Libertad Informática, un nuevo Derecho Fundamental en nuestra Constitución", *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía,* núm. 1, 2001.

ÁLVAREZ CIVANTOS, O.J.: *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades: (adaptación a la Ley 15/1999 de protección de datos de carácter personal y Reglamento de medidas de seguridad R.D. 994/1999),* Comares, 2001.

ÁLVAREZ HERNANDO, J.: "Relaciones laborales y protección de datos", Practicum Protección de Datos 2015, Aranzadi, 2014.

ÁLVAREZ-CIENFUEGOS SUAREZ, J.M.: La *defensa de la intimidad de los ciudadanos y la tecnología informática*, Aranzadi, 1999.

ALZAGA RUIZ, I.: "El uso por parte de la representación sindical de los medios informáticos propiedad de la empresa (Comentario a la Sentencia del Tribunal Constitucional 281/2005, de 7 de noviembre)", *Revista Española de Derecho del Trabajo*, núm. 132, 2006.

AMORÓS PÉREZ, F.: " La relación laboral especial de los discapacitados que trabajan en centros especiales de empleo (I): forma del contrato, capacidad para contratar como trabajador, tiempo de trabajo y salario" en VV.AA.: *La aplicación del derecho del trabajo en los centros especiales de empleo,* Tirant lo Blanch, 2009.

APARICIO SALOM, J.: "La calidad de los datos" en TRONCOSO REIGADA, A. (coord.): *Comentarios a la Ley Orgánica de protección de Datos*, Thomson-Civitas, 2010.

APARICIO SALOM, J.: *Estudio sobre la protección de datos*, Thomson-Reuters Aranzadi, 2013.

APARICIO TOVAR, J.: "Relación de trabajo y libertad de pensamiento en las empresas ideológicas", en *Lecciones de Derecho del Trabajo en homenaje a los profesores Bayón Chacón y Del Peso Calvo*, Universidad Complutense de Madrid, 1980.

APDCM: " Tratamiento de datos de salud con la finalidad de promover la adaptación de su puesto de trabajo", *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, núm. 40, 2009.

APDCM: "Tratamiento de datos de salud para adaptaciones curriculares" *Revista de la Agencia de Protección de datos de la Comunidad de Madrid*, núm. 34, 2008.

APDCM: *Principios y derechos de la protección de datos de carácter persona*l, Thomson Civitas, 2010.

APILLUELO MARTIN, M.: "Derecho de información del delegado sindical a las retribuciones de los trabajadores y derechos a la libertad sindical y a la protección de datos de carácter personal" *Revista Doctrinal Aranzadi Social*, núm. 28, 2011.

APILLUELO MARTÍN, M.: *La relación de trabajo del menor de edad*, CES, 1999.

AREITIO BERTOLÍN, J. Y AREITIO BERTOLÍN, T.: "Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación" *Revista Española de electrónica*, núm. 630, 2007.

ARENAS RAMIRO, M.: "La protección de datos personales en los países de la Unión Europea", Revista Jurídica de Castilla y León, núm.16, 2008.

ARENAS RAMIRO, M.: *El derecho fundamental a la protección de datos personales en Europa,* Dykinson, 2006.

ARESE, C.: "Empresas ideológicas o de tendencia" en VV.AA.: *Diccionario internacional de derecho del trabajo y de la seguridad social*, Tirant lo Blanch, 2014.

ARIAS DOMÍNGUEZ, A. Y RUBIO SÁNCHEZ, F.: *El derecho de los trabajadores a su intimidad,* Aranzadi, 2006.

ARIAS DOMÍNGUEZ, A.: "El "Outplacement" como método de lucha contra un desempleo muy cualificado" *Anuario de la Facultad de Derecho*, vol. 23, 2005.

ARIAS POU, M.: "El encargado del tratamiento y el documento de seguridad" en VV.AA.: *Derecho y Nuevas Tecnologías*, Univ. Deusto, 2011.

AUVERGNON, P.: "Acerca de la intermediación en el mercado de trabajo en Francia", *Revista Temas Laborales*, núm. 117, 2012, pp. 63-65.

BABSON, M.: "Monitoring Electronic Mail in the workplace: property versus privacy" en REMY NASH, J.: *Workplace Privacy*, Kluwer Law International, 2010.

BACARRIA MARTRUS, J.: "El caso whatsapp. Las aplicaciones de mensajería instantánea como medio de prueba en el procedimiento judicial", *Economist & Jurist,* Vol. 22, núm. 185, 2014, pp. 80-85.

BAJO GARCÍA, I.: La tutela judicial de los derechos fundamentales y libertades públicas, Boletín Laboral núm., 2013 disponible en http://www.elderecho.com /tribuna/laboral/derechos_fundamentales_de_los_trabajadores-libertades _publi cas_en_el_Orden_Social-leyreguladora_de_la_Jurisdiccion_Social-libertad _sin dical_11_594430003.html.

BALAGUER CALLEJÓN, F.: "Derecho y derechos en la Unión Europea", en CORCUERA ATIENZA, J. (coord.), *La protección de los derechos fundamentales en la Unión Europea*, Dykinson, 2002.

BALLESTER PASTOR, I.: "Sobre la expansión sostenida de la garantía de indemnidad retributiva del liberado sindical" *Revista Aranzadi Social*, núm. 13, 2010.

BARBANCHO TOVILLAS, F.: "Derecho a la información sobre retribuciones de sección sindical versus derecho a la intimidad y protección de datos personales en la Sociedad Estatal de Correos", *Revista Aranzadi Social*, núm. 30, 2007.

BARCELÓ, R.: "Transferencia internacional de datos personales" en VV.AA.: Protección de datos *comentarios a la LOPD y su reglamento de desarrollo*, Tirant lo Blanch, 2009.

BARNÉS VÁZQUEZ, J.: *Innovación y reforma en el Derecho Administrativo*, Ed. Derecho Global, 2006.

BARRIUSO RUIZ, C.: "Las redes sociales y la protección de datos hoy" *Anuario de la Facultad de Derecho*, núm. 2, 2009.

BAYLOS GRAU, A. Y VALDÉS DE LA VEGA, B.: "El efecto de las nuevas tecnologías en las relaciones colectivas de trabajo" en VV.AA.: *Nuevas Tecnologías de la información y comunicación y Derecho del Trabajo*, Bomarzo, 2004.

BAYLOS GRAU, A.: "Medios de prueba y derechos fundamentales. Especial referencia a la tutela de estos derechos" en AGUSTÍ JULIÁ, J.: *La prueba en el proceso laboral*, Cuadernos de derecho judicial, 1998.

BELLAVISTA A.: *Il controlo sui lavoratori*, Turín. Giappichelli, 1995.

BENAVENTE TORRES, I.: "La Reforma de la Intermediación Laboral por la Ley 35/2010", *Revista Trabajo,* núm. 24, 2011.

BENÍTEZ-DONOSO LOZANO, J.: "Sobre el reconocimiento de los derechos profesionales de los liberados sindicales: a propósito de la sentencia del Tribunal Constitucional 90/2008 de 21 de julio" *Revista de Derecho Social,* núm. 44, 2008.

BERNARDO JIMÉNEZ, I.: "Vigilancia de la salud de los trabajadores: Los reconocimientos médicos", *Revista Doctrinal Aranzadi Social*, núm. 20, 2003.

BETÉS DE TORO, A.: "El derecho de información y los principios legitimadores del tratamiento automatizado de los datos de carácter personal en la Directiva 95/46/CE, de 24 de octubre de 1995", *Actualidad Informática Aranzadi,* núm. 25, 1997.

BLASCO JOVER, C.: "Las novedades introducidas en la modalidad procesal de tutela de derechos fundamentales tras la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social", *Actualidad Laboral,* núm. 15-16, 2012.

BLASCO PELLICER, A.: "El deber empresarial de vigilancia de la salud y el derecho a la intimidad del trabajador" en VV.AA.: *Trabajo y Libertades Públicas*, Madrid, La Ley-Actualidad, 1999.

BLASCO PELLICER, C.: "Incidencia de las nuevas tecnologías de la información y la comunicación (TICS) en las reestructuraciones de las empresas", *Aranzadi Social*, núm.15, 2009.

BLAT GIMENO, F.: *Relaciones laborales y empresas ideológicas*, Ministerio de Trabajo y Seguridad Social, 1986.

BOURCIER, D.: *Inteligencia artificial y derecho*, Ed. UOC, 2003.

BRAUN, G.: "Le teletravail", *Droit Social* núm. 7-8, 1981.

BRONSTEIN, A. S.: "La protección de la vida privada en el lugar de trabajo", en *Anales del II Congreso Internacional de Derecho del Trabajo y de la Seguridad Social*, Isla Margarita (Venezuela), 2008.

BRU CUADRADA, E.: "La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad", *Revista de Internet, Derecho y Política*, núm. 5, 2007.

BUSTO LAGO, J.M.: "La Responsabilidad Civil de los responsables de ficheros de datos personales y de los encargados de su tratamiento", *Revista Doctrinal Aranzadi Civil-Mercantil,* núm. 5, 2006.

CALVO GALLEGO, F.J.: "Modalidades contractuales, dualidad en el mercado y reformas laborales en el bienio 2010 a 2012", *Documentación Laboral*, núm. 94, 2012.

CALVO GALLEGO, F.J.: "Test genéticos y vigilancia de la salud del trabajador", *Derecho y conocimiento*, núm. 2, 2002.

CALVO GALLEGO, F.J.: *Códigos éticos y derechos de los trabajadores: una aproximación a la práctica en las empresas españolas*, Bomarzo, 2008.

CALVO GALLEGO, F.J: *Contrato de trabajo y Libertad ideológica. Derechos fundamentales y organizaciones de tendencia* CES, Colección Estudios 1995.

CALVO GALLEGO, J.: "TIC y poder de control empresarial: reglas internas de utilización y otras cuestiones relativas al uso de Facebook y redes sociales" *Revista Doctrinal Aranzadi Social,* núm. 9, 2012.

CAMAS RODA, F.: "Las infracciones y sanciones administrativas del empresario en el orden social" *Estudios financieros. Revista de Trabajo y Seguridad Social*, núm. 254, 2004.

CAMPAL MARTÍNEZ, A.: "Libertad sindical y el uso de las nuevas tecnologías de la información y comunicación en el ejercicio de las libertades de expresión e información por los representantes de los trabajadores" *Revista General de Derecho del Trabajo y Seguridad Social*, núm. 27, 2011.

CAMPELO LÓPEZ, O.: "Los actos de encuadramiento en el sistema de la Seguridad Social: inscripción de empresas y afiliación, altas y bajas de los trabajadores" en MELLA MÉNDEZ, L. Y GARCÍA ROJO, A. (coord.): *Prácticas de la Seguridad Social,* La Ley, 2011.

CAMPUZANO LAGUILLO, A.B.: "Algunas consideraciones sobre la libertad informática y el derecho a la protección de datos de carácter personal en la jurisprudencia constitucional", *Revista Aranzadi de derecho y nuevas tecnologías*, núm. 1, 2003.

CAMPUZANO TOMÉ, H.: "Marco regulador de la protección de datos de carácter personal en las redes sociales digitales" *Actualidad Civil*, núm. 6, 2011.

CANALES GIL, A.: "Derecho de información en la recogida de datos" en Troncoso Reigado, A.: Comentarios a la Ley Orgánica de Protección de Datos, Thomson-Civitas, 2010.

CANALES GIL, A.: "Las competencias sancionadoras de la AEPD y el procedimiento sancionador: de nuevo sobre los principios de información y consentimiento" *Revista Jurídica de Castilla y León,* núm.16, 2008.

CANALES GIL, A: "La agencia española de protección de datos" en VV.AA: *Protección de datos de carácter personal en Iberoamérica: (II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala, 2-6 de junio de 2003)*, Tirant lo Blanch, 2005.

CANALES GIL, A; "La protección de datos como derecho fundamental", *Revista Jurídica de Castilla y León,* núm. 16, 2007.

CARDENAL CARRO, M.: "Desdramatizando el uso de internet en el trabajo" *Aranzadi Social*, núm.15, 2001.

CARDONA RUBERT M.B.: "Los datos del trabajador en las agencias de colocación: aplicación de la Ley 5/1992, de regulación del tratamiento automatizado de datos de carácter personal en las agencias de colocación", en VVAA.: *Inserción laboral: I Jornadas Andaluzas de Relaciones Laborales*, Universidad de Huelva, 1999.

CARDONA RUBERT, M.B.: "Derechos de acceso, rectificación, cancelación y oposición" en VV.AA*.: Protección de datos: comentarios a la LOPD y su reglamento de desarrollo*, Tirant lo Blanch, 2009.

CARDONA RUBERT, M.B.: "La utilización de las redes sociales en el ámbito de la empresa" *Revista de Derecho Social*, núm. 52, 2010.

CARDONA RUBERT, M.B.: "Redes sociales y contrato de trabajo" en VV.AA.: *Derecho y redes sociales*, Civitas, 2010.

CARDONA RUBERT, M.B.: Datos sanitarios y relación laboral, Tirant lo Blanch, 1999.

CARDONA RUBERT, M.B.: *Informática y contrato de trabajo*, Tirant lo Blanch, 1999.

CARDONA RUBERT, M.B.: Tutela de la intimidad informática en el contrato de trabajo. *Revista de Derecho Social*, núm.6, 1999.

CARRASCO POLAINO, R.: "Las redes sociales en las organizaciones y su aplicación en la comunicación tanto hacia el mercado como hacia sus miembros" en VV.AA.: *Retos empresariales en un nuevo entorno*, Netbliblo, 2010.

CARRIZOSA PRIETO, E.: "Las facultades de vigilancia y control en el centro de trabajo y su incidencia sobre el derecho a la intimidad de los trabajadores" en VV.AA.: *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación,* Tirant lo Blanch, 2014.

CASAS BAAMONDE, M. E. Y PALOMEQUE LÓPEZ, M. C.: "La ruptura del monopolio público de colocación: colocación y fomento del empleo", *Relaciones Laborales*, núm. 6-7, 1994.

CELAYA, J.: *La empresa en la web 2.0. El impacto de las redes sociales y las nuevas formas de comunicación online en la estrategia empresarial,* Gestión 2000, 2008.

CLIMENT RODRÍGUEZ, J. Y NAVARRO ABAL, Y.: "Oficinas virtuales de Empleo. El reto de universalizar los servicios públicos de empleo", *Revista Trabajo* núm. 24, 2011.

COELHO MOREIRA, T.: *A privacidade dos trabalhadores e as Novas Tecnologías de Informacao e Comunicacao: contributo para um estudo dos limites do poder de controlo electrónico do empregador,* Almedida, 2010.

COLÁS NEILA, E.: "Elementos para la construcción de una teoría general sobre el uso y control del correo corporativo" en VV.AA.: *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Bomarzo, 2004.

COLÁS NEILAS, E: *Derechos fundamentales del trabajador en la era digital: una propuesta metodológica para su eficacia,* Bomarzo, 2012.

CORDERO GORDILLO, V.: *Igualdad y no discriminación de las personas con discapacidad en el mercado de trabajo,* Tirant lo Blanch, 2011.

CRUZ VILLALON, J.: "Regulación y práctica del derecho de huelga en España: balance y propuestas normativas" *Revista del Instituto de Estudios económicos*, núm. 2-3, 2010.

CUADROS GARRIDO, M.E.: "El uso de whatsapp en las relaciones laborales", *Revista Española de Derecho del Trabajo*, núm. 171, 2014.

DAGNINO, E.: "Social recruiting: una novità da perfezionare" publicado en *Conquiste del Lavoro*, el 21 de octubre de 2014, disponible en www.bolletino adapt.it.

DATTNER, B.: "El uso y el mal uso de los test de personalidad", *Revista Capital Humano*, núm.182 (Especial selección de personal), 2004.

DAVARA RODRÍGUEZ, M.A.: "Las medidas de seguridad de los datos" *Revista técnica especializada en administración local y justicia municipal,* núm.15-16. 2010.

DAVARA FERNÁNDEZ- MARCOS, I.: *Hacia la estandarización de la protección de datos de carácter personal,* La Ley, 2011.

DAVARA RODRÍGUEZ, M.A.: "Acerca de los principios del consentimiento y calidad de datos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD)", *Revista técnica especializada en administración local y justicia municipal*, núm. 2, 2009.

DAVARA RODRÍGUEZ, M.A.: "Intercambio de mensajes por Internet: el caso Whatsapp", *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, núm .7, 2014.

DAVARA RODRÍGUEZ, M.A.: "La nueva Ley Orgánica de protección de datos de carácter personal", en VV.AA.: *XIII Encuentro sobre informática y Derecho*, Aranzadi, 2000.

DAVARA RODRÍGUEZ, M.A.: *La protección de datos en Europa*, *principios, derechos y procedimiento,* Universidad Pontificia de Comillas, 1998.

DAVARA RODRÍGUEZ, M.A.: *Seguridad de los datos, nuevas tecnologías, sociedad y trabajo*, FUNDESCO, Madrid, 1991.

DAVARA RODRÍGUEZ, M.A.: "La relación entre los artículos 28.1 CE (Libertad sindical) y 18.4 CE (tratamiento automatizado de datos de carácter personal), desde la óptica de la llamada "protección de datos personales", *Repertorio Aranzadi del Tribunal Constitucional,* vol. IV, parte Estudio, 1998.

DE LA CASA QUEMADA, S.: "I.as empresas de recolocación (outplacement) y nuevos derechos del trabajador a la prevención del desempleo", *Trabajo: Revista andaluza de relaciones laborales*, núm. 20, 2007.

DE LA VILLA GIL, L.E.: "La Carta de los Derechos fundamentales de la Unión europea", *Revista del Ministerio de Trabajo y Asuntos Sociales*, núm. 32, 2001.

DE MIGUEL, N.: *Tratamiento de datos personales en el ámbito sanitario. Intimidad versus interés público*, Tirant lo Blanch, Valencia, 2004.

DE PABLOS, S.: "El impacto 2.0 en la búsqueda y selección de profesionales con talento", *Revista Capital Humano,* núm. 248, 2010.

DE TISSOT, O.: "Internet et contrat de travail. Les incidences de la connexión á Internet sur les rapports employeur-salariés", *Droit Social*, núm. 2, 2000.

DE VAL TENA, A.L.: *"*Las empresas de tendencia ante el Derecho del Trabajo: libertad ideológica y contrato de trabajo", *Proyecto social: relaciones laborales*, núm. 2, 1994.

DE VICENTE PACHÉS, F.: "El control empresarial del ordenador. A propósito de la Sentencia del Tribunal Supremo -unificación de doctrina- de 26 de septiembre de2007", *Tribuna Social* núm. 214, 2008.

DE VICENTE PACHÉS, F.: *"*Protección de datos personales y agentes intermediarios de colocación; la tutela de la libertad informática-intimidad del demandante de empleo*"*, *Revista del Consejo Económico y Social (CES),* núm. 64, 2012.

DE VICENTE PACHÉS, F: *El derecho del trabajador al respeto de su intimidad*, CES, 1998.

DEL CASTILLO VÁZQUEZ, I.C.: "Transparencia, acceso a la documentación administrativa y protección de datos de carácter personal", *Foro Nueva Época*, núm. 6, 2007.

DEL CASTILLO VÁZQUEZ, I.C.: *Protección de datos: cuestiones constitucionales y administrativas*, Thomson-Civitas, 2007.

DEL PESO NAVARRO, E. Y RAMOS GONZÁLEZ, M.A.: *Confidencialidad y seguridad en la información: la LORTAD y sus implicaciones socioeconómicas*, Díaz-Santos, Madrid, 1994.

DEL PESO NAVARRO, E.: "La figura del responsable del fichero de datos de carácter personal en la L.O.R.T.A.D", *Informática y derecho: Revista iberoamericana de derecho informático*, núm. 6-7, 1994.

DEL REY GUANTER, S.: "Nuevas técnicas probatorias, obtención ilícita de la prueba y derechos fundamentales en el proceso laboral", *Revista Española de Derecho del Trabajo,* núm. 37, 1989.

DEL REY GUANTER, S.: "Tratamiento automatizado de datos de carácter personal y contrato de trabajo. Una aproximación a la "intimidad informática" del trabajador", *Revista Relaciones Laborales,* núm. 2, 1993.

DEL REY GUANTER, S.: *Relaciones laborales y nuevas tecnologías*, La Ley, 2005.

DEL VAL PUERTO, E.: "Zonas de incertidumbre: ámbito de aplicación" en TRONCOSO REIGADA, A, (dir): *Transparencia administrativa y protección de datos personales*, Civitas, 2008.

DEL VALLE, J.M: "El derecho a la intimidad del trabajador durante la relación de trabajo", *Actualidad Laboral*, núm. 39, 1991.

DESDENTADO BONETE A. Y MUÑOZ RUIZ, A.B.: "Protección de datos y contrato de trabajo" *Revista Justicia Laboral*, núm.46, 2011.

DESDENTADO BONETE, A. Y MUÑOZ RUIZ, A.B.: *Control informático, video vigilancia y protección de datos en el trabajo,* Lex Nova, 2012.

DESDENTADO BONETE, A. Y MUÑOZ RUIZ, B.: "Trabajo, video vigilancia y controles informáticos: un recorrido por la jurisprudencia" *Revista General de Derecho del Trabajo y de la Seguridad Social,* núm.39, 2014.

DÍAZ REVORIO, F.J.: "Derecho de información en la recogida de datos. Una perspectiva constitucional" en VV.AA.: *Comentarios a la Ley Orgánica de Protección de datos de carácter personal*, Thomson-Civitas, 2010.

DÍAZ LLAIRÓ, A*.: El talento está en la red*, Lid Editorial, 2011.

DÍAZ RODRÍGUEZ, J.M.: "Detectives en el ámbito laboral: poder empresarial y prueba judicial", *Actualidad Laboral*, núm. 7, 2011.

DÍAZ RODRÍGUEZ, J.M.: "Intimidad y privacidad sindical frente al control empresarial" *Comunicación presentada al XXIV Congreso nacional de Derecho del Trabajo y Seguridad Social*, Pamplona, 2014, pág.7.

DOMÍNGUEZ MARTÍN, A.: "Las agencias de colocación (o la privatización del desempleo)", *Lex Nova: La Revista,* núm. 63, 2011.

DONOVAN, C.: "Data protection and the retention of personal data: how long is too long?" Computer Law and Security Report, vol. 20, Issue 6, 2004.

DORREGO DE CARLOS, A; "La reforma de la intermediación laboral en la Ley 35/2010: perspectiva desde el sector de las ETT", *Diario la Ley* núm. 7488, 2010.

ENDEMAÑO AROSTEGUI, J.M.: "La Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública de creación de la Agencia

Vasca de Protección de Datos", en VV.AA. *Estudios sobre administraciones públicas y protección de datos personales*, AGPDCM, 2006.

ESTEVE PARDO, A.: "Uso de datos personales por parte de google y facebook y protección de la intimidad en Europa Y Estados Unidos" en VV.AA.: *Internet, Derecho y Política. Regulating Smart Citie*. Actas del XI Congreso Internacional, Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona 2-3 Julio, 2015. Barcelona: UOC-Huygens Editorial.

FALCÓN Y TELLA, F.: "Medidas de seguridad aplicables a ficheros y tratamientos de datos de carácter personal", *Foro Nueva Época*, núm.8, 2008.

FATÁS, J.M. Y GARCÍA SANZ, J.M.: "Comentario al art. 5 del Reglamento de desarrollo de la LO 15/1999, de Protección de Datos de Carácter Personal", en FERIA BASILIO, I.: *La tutela del patrimonio genético del trabajador*, Bomarzo, 2013.

FERNÁNDEZ DOMÍNGUEZ, J.J. Y RODRÍGUEZ ESCANCIANO, S.: *Utilización y control de datos laborales automatizados*, Agencia de Protección de Datos, 1997.

FERNÁNDEZ DOMÍNGUEZ, J.J.: "Test de alcohol y drogas en el trabajo: la selección de la prueba más respetuosa con los derechos fundamentales del trabajador" en VV.AA. *Los derecho fundamentales inespecíficos en la relación laboral y en materia de protección social*, Cinca, 2014, disponible en CD.

FERNÁNDEZ GARRIDO, J.: "Los Retos de los Servicios Públicos de Empleo: Una visión externa", *Revista Trabajo*, núm. 24, 2011.

FERNÁNDEZ LÓPEZ, J.M.: "Algunas reflexiones sobre los aspectos generales que regula el reglamento de desarrollo de la LOPD", *Revista Española de Protección de Datos*, núm.3, 2007.

FERNÁNDEZ LÓPEZ, J.M.: "La nueva Ley de Protección de Datos de Carácter Personal de 13 de diciembre de 1999. Su por qué y sus principales novedades", *Actualidad Informática Aranzadi*, núm. 34, 2000.

FERNÁNDEZ LÓPEZ, M.F.: "Libertad ideológica y prestación de servicios", *Relaciones Laborales*, Tomo II, 1985.

FERNÁNDEZ MÁRQUEZ, O. Y GARCIA MURCIA J.: "Infracciones extra sistemáticas del empresario en materia social" *Revista del Ministerio de Trabajo e Inmigración,* núm. 78, 2008.

FERNÁNDEZ MÁRQUEZ, O.: "La utilización por los trabajadores de los bienes de la empresa: un enfoque desde el derecho de propiedad", *Revista española de Derecho del Trabajo*, núm. 148, 2010.

FERNÁNDEZ RODRÍGUEZ, C. Y MARTÍN MARTÍN, M.P.: "Los discursos sobre la modernización de los Servicios Públicos de Empleo: ¿hacia una nueva forma de gobernanza?", *Revista Política y Sociedad*, núm. 51, 2014.

FERNÁNDEZ RODRÍGUEZ, J: *Secreto e intervención de las comunicaciones en internet*, Thomson Civitas, 2004.

FERNÁNDEZ SALMERÓN, M.: *La protección de datos en la administración pública*, Civitas, 2003.

FERNÁNDEZ VILLAZÓN, L.A.: "Tratamiento automatizado de datos personales en los procesos de selección de trabajadores", *Revista Relaciones Laborales,* núm. 1, 1994.

FERNÁNDEZ VILLAZÓN, L.A.: "Los derechos de los trabajadores frente al tratamiento de datos personales. Comentario a la directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos", *Relaciones Laborales*, núm. 2, 1996.

FERNÁNDEZ VILLAZÓN, L.A.: *Las facultades empresariales de control de la actividad laboral*, Thomson Aranzadi, 2003.

FERNÁNDEZ-ALLER, C.: "Algunos retos de la protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en nube (cloud computing)" Revista de Derecho UNED, núm. 10, 2012.

FREIXAS GUTIÉRREZ, G.: *La protección de los datos de carácter personal en el derecho español*, Bosch, 2000.

FUENTES RODRÍGUEZ, F.: "Contenido de la libertad sindical: Compatibilidad de la condición de liberado sindical con la ocupación de una plaza en situación especial en activo" *Temas Laborales*, núm. 55, 2000.

GALA DURÁN, C.: "La Directiva sobre empresas de trabajo temporal y su impacto en España", *Temas Laborales: Revista Andaluza de Trabajo y Bienestar Social*, núm. 102, 2009.
GALÁN JUÁREZ, M.: "Comentario de la Sentencia 292/2000 de 30 de noviembre. Protección de datos de carácter personal. Los derechos civiles individuales" en DORREGO DE CARLOS, A.:*25 años de Jurisprudencia Constitucional*, Grupo Difusión, 2007.

GAMERO, R.: "Servicios basados en redes sociales, la Web 2.0", *Boletín de la Sociedad de la Información: Tecnología e Innovación*, vol. 6, núm. 9, 2006.

GARCÍA COCA, O.: "Algunas cuestiones sobre las posibilidades y limitaciones de supervisión del ordenador del trabajador por parte del empresario", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 34, 2014.

GARCÍA GARNICA, M.C.: "La protección de los datos relativos a la salud de los trabajadores (a propósito de la STC 202/1999 de 8 de noviembre)", *Derecho Privado y Constitución*, núm.14, 2000.

GARCÍA GIL, M.B.: "Mecanismos de intermediación laboral tras la reforma laboral de 2010; principales modificaciones", *Revista Aranzadi Doctrinal*, núm. 11, 2011.

GARCÍA MURCIA, J. Y MARTÍNEZ MORENO, C.: *Los derechos de información en el contrato de trabajo*, Tirant lo Blanch, 2001.

GARCÍA MURCIA, J.: "El trabajo de los incapacitados", *Tribuna Social*, núm. 91, 1998.

GARCÍA MURIAS, R.: "El Programa Erasmus y la Red Eures incidencia en la movilidad académico-profesional en el contexto europeo" en VV.AA.: *Orientación profesional: nuevos escenarios y perspectivas*, Biblioteca Nueva, 2009.

GARCÍA NINET, J.I.: "Derecho a la indemnidad económica y profesional: del liberado sindical y promoción laboral. Breves cuñas en torno a la STC 90/2008, de la Sala Primera, de 21 de julio", *Tribuna Social: Revista de Seguridad Social y laboral*, núm. 215, 2008.

GARCÍA NINET, J.I.: "Intermediación laboral y agencias de colocación y de recolocación privadas: comentario al Real Decreto 1796/2010, de 30 de diciembre", *Revista Española de Derecho del Trabajo y Seguridad Social*, núm. 24, 2011.

GARCÍA NINET, J.I.: "Los derechos de los trabajadores a la protección de la seguridad y la salud en el trabajo y las obligaciones empresariales sobre estas mismas materias" en VV.AA; *Lecciones sobre la Ley de Prevención de Riesgos Laborales*, Servicio de Publicaciones Universitat Jaime I, 1997.

GARCIA NINET, J.I.: "Sobre el uso y el abuso del teléfono, del fax, del ordenador de la empresa en lugar y tiempo de trabajo. Datos para una reflexión en torno a las nuevas tecnologías" *Tribuna Social*, núm.127, 2001.

GARCÍA NINET, J.I.: "Sobre el uso y el abuso del teléfono, del fax, del ordenador y del correo electrónico de la empresa para fines particulares en lugar y tiempo de trabajo. Datos para una reflexión en torno a las nuevas tecnologías", *Tribuna Social*, núm. 127, 2001.

GARCÍA QUIÑONES, J.C.: "El concepto jurídico laboral de discapacitado" en VALDÉS DAL-RE, F. Y LAHERA FORTEZA, J.: *Relaciones laborales de las persona con discapacidad*, Ed. Biblioteca Nueva, 2005.

GARCÍA ROMERO, B.: "La protección jurídico-laboral de los menores", *Revista Aranzadi Social,* núm. 10, 2001.

GARCÍA VELARDE, M.: "Los elementos esenciales del contrato de trabajo: visión jurisprudencial", *Documentación Laboral*, núm. 45, 1995.

GARCÍA VIÑA, J.: *La buena fe en el contrato de trabajo,* CES, 2001.

GARCÍA-BERRIO HERNÁNDEZ, T.: *Informática y libertades: La protección de datos personales y su regulación en España y Francia,* Servicio de publicaciones de la Universidad de Murcia, 2003.

GARCÍA-NÚÑEZ SERRANO, F.: "La regularización sobre protección de datos personales y su incidencia en el ámbito laboral", *Aranzadi Social*, núm. 5, 2000.

GARCÍA-PERROTE ESCARTÍN, I. Y MERCADER UGUINA, J.: "Conflicto y ponderación de los derechos fundamentales de contenido laboral" en VV.AA*: El modelo social en la Constitución Española 1978*, Ministerio de Trabajo e inmigración, Subdirección General de Publicaciones, 2003.

GARCÍA-PERROTE ESCARTÍN, I.: "Convenio colectivo y contrato de trabajo. Y sobre los derechos constitucionales inespecíficos del trabajador" en ROJO TORRECILLA E.: *Las reformas laborales de 1994 y 1997,* Marcial Pons, 1998.

GARCÍA-PERROTE ESCARTIN, I.: "Derecho de huelga y libertad de empresa" *Revista Jurídica de Castilla y León*, núm. 5, 2005.

GARRIDO PÉREZ, E.: "El tratamiento comunitario de la discapacidad", *Revista Temas Laborales*, núm. 59, 2001.

GARRIGA DOMÍNGUEZ, A.: *Tratamiento de datos personales y derechos fundamentales*, Dykinson, 2009.

GAY FUENTES, C.: *Intimidad y tratamiento de datos en las Administraciones Públicas,* Universidad Complutense, Madrid, 1995.

GIL PLANA, J.: "Control empresarial del uso personal por el trabajador de los medios tecnológicos de trabajo. Comentario a la STC 170/2013, de 7 de octubre", *Nueva Revista Española de Derecho del Trabajo*, núm. 164, 2014.

GIRARD, A. Y FALLERY, B.: "E-recruitment: new practices, new issues. An exploratory study", en *Proceedings of the Third International Workshop on Human Resource Information Systems*, INSTICC Press, Milan, 2009.

GOERLICHPESET, J. M.: *"*Reformas en materia de empleo y de empresas de trabajo temporal" en VV.AA, *La Reforma Laboral en el Real Decreto-Ley 10/2010,* Valencia, Tirant lo Blanch, 2010.

GÓMEZ-MILLÁN HERENCIA, M.J.: *Colectivos destinatarios de las políticas selectivas de empleo,* Laborum, 2011.
GÓMEZ-MILLÁN HERENCIA, M.J: *"*Extinción del contrato de trabajo. El despido por razones ideológicas en la Administración Pública*", Temas Laborales* núm. 108, 2001.

GONZÁLEZ BARTUREN, J.: "Bases de datos de recursos humanos y la Ley Orgánica de protección de Datos de Carácter Personal: Una adaptación lógica" *Boletín de Estudios Económicos*, vol. 60, núm.185, 2005.

GONZÁLEZ DÍAZ, F.A.: "Una interpretación sobre los límites a la realización de reconocimientos médicos a los trabajadores" *Aranzadi Social*, núm.52, 2011.

GONZÁLEZ FIERRO, C.: "El deber empresarial de garantizar la vigilancia periódica de la salud de los trabajadores: obligatoriedad versus voluntariedad", *Revista Información Laboral*, núm. 8, 2004.

GONZÁLEZ NAVARRO, F.: "La relación jurídica de disposición de datos de carácter personal" en VV.AA.: *El derecho a la intimidad y a la privacidad y las administraciones públicas*, Escola Galega de Administración Pública, 1999.

GONZÁLEZ ORTEGA, S. "El conflicto entre los derechos fundamentales del trabajador y la libertad de empresa: el necesario tránsito desde el juicio de proporcionalidad al juicio de ponderación", *Revista Chilena de Derecho del Trabajo*, vol. 3, núm. 6, 2012.

GONZÁLEZ ORTEGA, S. Y GÓMEZ-MILLÁN HERENCIA, M.J.: "Forma y duración" en VV.AA.: *Las empresas de trabajo temporal: estudio de su régimen jurídico,* Comares, 2014.

GONZÁLEZ ORTEGA, S.: "La informática en el seno de la empresa. Poderes del empresario y condiciones de trabajo" en VV.AA: *Nuevas tecnologías de la información y la comunicación y Derecho del trabajo*, Bomarzo, 2004.

GONZÁLEZ TAPIA, M.L.: "El derecho de oposición" *Datos personales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, núm. 25, 2007.

GONZÁLEZ TAPIA, M.L: "España: El encargado del tratamiento de datos" *AR: Revista de derecho informático*, núm. 110, 2007.

GOÑI SEÍN, J.L.: "Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y archivo de datos", en VV.AA.: *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Albacete Bomarzo, 2004.

GOÑI SEÍN, J.L.: "Análisis genéticos en el ámbito laboral", *Revista de Derecho Social*, núm. 47, 2009.

GOÑI SEIN, J.L.: "Valor jurídico de los códigos de conducta" en GOÑI SEIN, J.L. (coord.): *Ética empresarial y códigos de conductas*, La ley, 2011.

GOÑI SEÍN, J.L.: "Vigilancia de la salud versus protección de la intimidad del trabajador", en HORTAL IBARRA, J.C*.: Protección penal de los derechos de los trabajadores,* Edisofer, 2009.

GOÑI SEÍN, J.L.: *El respeto a la esfera privada del trabajador. Un estudio sobre los límites del poder de control empresarial*, Civitas, 1988.

GOÑI SEÍN, J.L.: Los derechos fundamentales inespecíficos en la relación laboral individual: ¿necesidad de una reformulación?, en VV.AA.: *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social,* XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, Cinca, 2014.

GOÑI SEIN, J.L: "Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos", *Justicia Laboral*, núm. 39, 2009.

GUALDA ALCALÁ, F.J.: "La protección de los datos personales en las relaciones laborales" en *Estudios de Doctrina Judicial III*, Bomarzo, 2009.

GUASCH PORTAS, V.: "Transferencia internacional de datos de carácter personal", *Revista de Derecho de la Uned,* núm. 11, 2012.

GUDE FERNÁNDEZ, A.: "La video vigilancia laboral y el derecho a la protección de datos de carácter personal", *Revista de Derecho Político*, núm.91, 2014.

GUERRERO PICÓ, M.C.: *El impacto de Internet en el derecho a la protección de datos de carácter personal*, Thomson-Civitas, 2006.

GUERRERO VIZUETE, E.: "El plan de recolocación externa de los trabajadores excedentes: un nuevo instrumento de lucha contra el desempleo" en CABEZA PEREIRO, J. (coord.): *Políticas de empleo*, Aranzadi, 2013.

GUICHOT REINA, E.: *Datos personales y Administración Pública*, Thomson-Civitas, 2005.

GUICHOT REINA, E.: *Publicidad y privacidad de la información administrativ*a, Thomson-Civitas, 2009.

GUICHOT REINA, E.: T*ransparencia y acceso a la información en el Derecho Europeo*, Ed. Derecho Global, 2011.

GUTIÉRREZ MARTÍNEZ, R.: *La administración pública electrónic*a, Civitas, 2009.

GUTIÉRREZ PÉREZ, M.: "Prohibición expresa del uso privado del ordenador de la empresa como fundamento para su control", *Revista española de Derecho del Trabajo*, núm. 165, 2014.

HERBERT, A.S.: "What computers mean for man and society", en VV.AA. *Microelectronics revolutions*, Forrester. T. ed.

HEREDERO HIGUERAS, M.: "La nueva Ley alemana federal de protección de datos". *Boletín Oficial del Ministerio de Justicia*, núm. 1630. pág.130, disponible en http://www.mjusticia.gob.es/cs/.

HEREDERO HIGUERAS, M.: *La Directiva Comunitaria de Protección de Datos de Carácter Personal*, Aranzadi, 1997.

HERNÁNDEZ CORCHETE, J.A.: "El derecho de los ciudadanos a relacionarse con las administraciones públicas utilizando los medios electrónicos y los derechos complementarios que delimitan su alcance" en PIÑAR MAÑAS, J.L. (coord.): *Transparencia, acceso a la información y protección de datos*, Reus, 2014.

HERNÁNDEZ I MORENO, J.X.: "La Ley 5/2002, de 19 de abril, de creación de la Agencia Catalana de Protección de Datos." en VV.AA. *Estudios sobre administraciones públicas y protección de datos personales*, AGPDCM, 2006.

HERNÁNDEZ LAHOZ, M. Y GIL LACRUZ, M.: "Origen y evolución de las empresas de Trabajo Temporal", *Revista Capital Humano*, año nº 24, núm. extra 257, 2011.

HERNÁNDEZ LAHOZ, M. Y GIL LACRUZ, M.: "Proceso y técnicas de selección" *Revista Capital Humano*, Año nº 24, Nº Extra 257, 2011.

HERNÁNDEZ LÓPEZ, J.M*.: El derecho a la protección de datos en la Doctrina del Tribunal Constitucional*, Thomson-Reuters Aranzadi, 2013.

HERRÁN ORTIZ, A.I.: *El derecho a la intimidad en la Nueva Ley Orgánica de protección de datos personales*, Dykinson, 2002.

HERRÁN ORTIZ, A.I.: *La violación de la intimidad en la protección de datos personales*, Dykinson, 1999.

HERRERO DE EGAÑA, J.M.: "Intimidad, tributos y protección de datos personales", *Indret (Revista para el análisis del Derecho)*, núm. 2, 2007.

HIERRO HIERRO, F.J.: "Una aproximación al sistema de red de la Tesorería General de la Seguridad Social", *Revista Aranzadi Social*, núm. 2, 2003.

ICHINO, P.: "Telelavoro e normativa: quali prospettive di adequamento" en VV.AA *Telelavoro i miti e le prospettive concrete per l'Italia*, Giuffré, 1989.

INAP: *Libro Blanco sobre la administración electrónica y la protección de datos,* Ministerio de Administraciones Públicas, 2001.

JEFFERY, M.: "Derecho del trabajo en la sociedad de la información" en VV.AA: *Derecho y nuevas tecnologías,* UOC, 2009.

LAHERA FORTEZA, J.: "Acceso al mercado de trabajo y contratación de los discapacitados" en en VALDÉS DAL-RE, F. Y LAHERA FORTEZA, J.: *Relaciones laborales de las personas con discapacidad*, Ed. Biblioteca Nueva, 2005.

LÁZARO SÁNCHEZ, J.L: "Las agencias de colocación" en VV.AA: *Estudios en torno a la reforma laboral 2012*, Ed. Punto Rojo, 2013.

LEE, I., "E-recruiting: Opportunities and challenges", *Information Management*, vol. 19, núm. 3-4, 2006.

LEENES, R.:" ¿Quién controla la nube? *IP Revista de Derecho, Internet y Política,* núm. 11, 2010.

LESMES SERRANO, C (coord.): *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia,* Lex Nova, 2008.

LLEO CASANOVA, B.: "Novedades en materia de contratación laboral introducidas por el RD-Ley 4/2013, de 22 de febrero, de medidas de apoyo al emprendedor y de estímulo del crecimiento y de la creación de empleo" *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 34, 2013.

LLORENS ESPADA, J.: "El uso de facebook en los procesos de selección de personal y la protección de los derechos de los candidatos" *Revista de Derecho Social*, núm.68, 2014.

LÓPEZ ANIORTE, M.C.: "Límites constitucionales al ejercicio del poder directivo empresarial mediante el uso de las TIC y otros medios de vigilancia y seguridad privada en el ordenamiento jurídico español", *Policía y Seguridad Pública,* vol.1, núm. 4, 2014.

LÓPEZ ANTUÑA, J.: «Pulsar "Me gusta" en Facebook: Despido Nulo y Riesgos del uso de Whatsapp en la comunicación abogado cliente», *Revista del Consejo General de Colegios Oficiales de Graduados Sociales*, núm. 29, 2014.

LÓPEZ INSUA, B.M.: "El control del uso correcto del subsidio por incapacidad temporal: los supuestos de pérdida o suspensión", *Revista Trabajo y Seguridad Social (CEF)*, núm. 394, 2015.

LÓPEZ RAMÓN, F.: *La Agencia de protección de datos como Administración independiente* en Jornadas sobre protección de datos, AEPD, 1996.

LÓPEZ-ROMERO GONZÁLEZ, M.P.: "La Red EURES: puesta en contacto de ofertas y demandas de empleo en Europa", *Información laboral. Legislación y convenios colectivos,* núm. 22, 2003.

LUJAN ALCARAZ, J.: "Protección de datos de carácter personal y contrato de trabajo", *Revista Doctrinal Aranzadi Social,* núm. 7, 2003, pág.10.

LUJAN ALCARAZ, J.: "Uso y control en la empresa de los medios informáticos de Comunicación" *Aranzadi Social*, núm.3, 2001.

MAGALLÓN ORTÍN, M.: "Intercambio electrónico de dato en materia de afiliación y recaudación de Seguridad Social (Proyecto RED)", *Revista de Trabajo y Seguridad Social*, núm. 18, 1995.

MALUQUER DE MOTES I BERNET, C.J.: "Códigos de conducta y buenas prácticas en la gestión de datos personales" en LLÁCER MATACÁS, M.R.: *Protección de datos personales en la sociedad de la información y la vigilancia,* La Ley, 2011.

MARIN ALONSO, I.: *El poder de control empresarial sobre el uso del correo electrónico en la empresa. Su limitación en base al secreto de las comunicaciones*, Tirant lo Blanch, 2005.

MAROÑO OTERO, E.: "¿Cómo están afectando las redes sociales al mercado laboral en España?", *Revista Capital Humano*, núm. 287, 2014.

MARTIN PARDO DE VERA, M.: "Principios de la protección de datos: seguridad de los datos. Aplicación de los niveles de seguridad (1ª y 2ª parte)", en TRONCOSO REIGADO, A (coord.): C*omentario a la Ley Orgánica de protección de datos de carácter personal*, Thomson-Civitas, 2010.

MARTÍN VALVERDE (COORD.), A.: *Derecho del Trabajo*, Tecnos, 2012.

MARTIN-CASALLO LÓPEZ, J.J.: "Implicaciones de la Directiva sobre protección de datos en la normativa española", *Actualidad Informática Aranzadi,* núm.20, 1996.

MARTÍNEZ MARTÍNEZ, R.: *Protección de datos: Comentarios al reglamento de desarrollo de la LOPD*, Tirant lo Blanch, Valencia, 2009.

MARTINEZ FONS, D.: "Tratamiento y protección de datos de los trabajadores en la relación de trabajo" en VV.AA.: *Derecho Social y Nuevas Tecnologías*, CGPJ, 2005.

MARTÍNEZ LUCAS, J.A.: "El alta de los trabajadores en la Seguridad Social", Revista General de Derecho, núm.625-626, 1996.

MARTÍNEZ MARTÍNEZ, R.: "El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Aspectos claves", *Revista jurídica de Castilla y León*. núm. 16, 2008.

MARTÍNEZ SÁNCHEZ, M.: "Creación, notificación e inscripción registral de ficheros de titularidad privada: Título IV. Disposiciones Sectoriales. Cap. II. Ficheros de Titularidad Privada. Artículos 25 y 26" en TRONCOSO REIGADO, A (coord.): C*omentario a la Ley Orgánica de protección de datos de carácter personal*, Thomson-Civitas, 2010.

MARTINOTTI, G.: "Privacy e statuto dell'informazione" *Banchedati, telemática e diritti della persona,* Cedam, 1984.

MARZO PORTERA, A.: "La Agencia Española de Protección de Datos" en ALMUZARA ALMAIDA, C. (coord.): *Estudio práctico sobre la protección de datos de carácter personal*, Lex Nova, 2005.

MARZO PORTERA, A.: "Privacidad y cloud computing, hacia dónde camina Europa", *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche*, Vol. I, núm. 8 , 2012.

MATEU CARRUANA, M.J.: "Facultades de control fuera del centro de trabajo: medidas de control sobre las conductas extralaborales del trabajador"*, Tribuna Social*, núm. 169, 2005.
MELLA MÉNDEZ, L.: "La protección de los menores en el derecho del trabajo: reflexiones generales", *Revista Aranzadi Social*, núm. 13, 2008.

MENÉNDEZ SEBASTIÁN, P.: "Protección de datos personales del trabajador (Directiva 95/46/CE)" en VV.AA: *La transposición del Derecho Social Comunitario al ordenamiento español,* Ministerio de Trabajo y Asuntos Sociales, 2005.

MENENDEZ SEBASTIÁN, P.: *Aptitud legal y capacidad en el contrato de trabajo*, CES (España), 2003.

MERCADER UGUINA, J. R.: *Derecho del Trabajo, nuevas tecnologías y sociedad de la información*, Lex Nova, 2002.

MESANZA LEGARDA, S.: "*Efectos de la protección de datos de carácter personal en la gestión de recursos humanos"* Congreso Internacional de Gestión de RRHH en Administración Pública, 2007.

MING TING-DING, J Y DÉNIZ DÉNIZ, M.C.: "La selección del personal como un proceso ético y eficiente: el caso de la entrevista personal" en AYALA CALVO, J.C.(coord.).: Conocimiento, innovación y emprendedores : camino al futuro, Universidad de la Rioja, 2007.

MIRALLES, R: "Cloud computing y protección de datos de carácter personal" *Revista de Derecho, Internet y Política,* núm. 11, 2010.

MITJANS PERELLÓ, E.: *"*La experiencia de la Agencia Catalana de Protección de Datos*"* en VV.AA. *Estudios sobre comunidades autónomas y protección de datos personales,* AGPDCM, 2006.

MOLE, A.: "Au delá de la informátique et libertés", *Revista Droit Social*, núm.6, 1992.

MOLINA NAVARRETE, C.: "Derecho con mirada de mujer: la solución al conflicto de conciliación de la vida laboral y familiar en la STC 3/2007, de 15 de febrero", *Diario La Ley*, año XXVIII, núm. 6681, 2007.

MONEREO PÉREZ J.L Y MORENO VIDA, N.: "Las empresas de trabajo temporal en el marco de las nuevas formas de organización empresarial", *Revista Española del Ministerio de Trabajo y Asuntos Sociales*, núm. 48, 2004.

MONEREO PÉREZ, J.L.: *Los derechos de información de los representantes de los trabajadores*, Madrid (Civitas), 1992.

MONTOYA MELGAR, A.: "Nuevas tecnologías y buena fe contractual (Buenos y malos usos del ordenador en la empresa)" *Revista Relaciones Laborales*, núm.5-6, 2005.

MONTOYA MELGAR, A.: *La buena fe en el Derecho del Trabajo*, Tecnos, 2001.

MORAES REGO, N.: *La contribución del poder judicial a la protección de los derechos humanos de la tercera generación*, Ediciones Salamanca, 2014.

MORATO GARCÍA, R.: "El impacto de las redes sociales virtuales en los procesos de selección de trabajadores" Comunicación presentada al X Congreso Europeo de Derecho del Trabajo y de la Seguridad Social, Sevilla, 2011, disponible en: http://www.aedtss.com/images/stories/documentos/congreso europeo comunicaciones /1/106morato_garcia.pdf).

MORALES VALLEZ, C.: *Extincion del contrato de trabajo: causas objetivas y disciplinarias, el fogasa*, Colex, 2014.

MORENO BOTELLA, G.: *La libertad de conciencia del trabajador en las empresas ideológicas confesionales,* Fundación Universitaria Española, 2003.

MORENO DE VEGA Y LOMO, F.: "El nuevo régimen jurídico de las agencias de colocación", *Actualidad Laboral,* núm. 18, 2011.

MORENO GARCÍA, A.: "Buena fe y derechos fundamentales en la jurisprudencia del Tribunal Constitucional", *Revista Española de Derecho Constitucional*, núm. 38, 1993.

MORENO VIDA, N.; "Novedades en materia de modalidades contractuales: contrato indefinido para pequeñas empresas, trabajo a tiempo parcial y trabajo a distancia" *Revista Temas Laborales,* núm. 115, 2012.

MOTILLA DE LA CALLE, A.: "El derecho a discriminar en las relaciones laborales excepciones a la prohibición general de discriminar por motivos ideológicos o religiosos en Europa", *Revista Española de Derecho del Trabajo y de la Seguridad Social,* núm. 158, 2013.

MUÑOZ RUIZ, A.B. Y MORENO SOLANA, A.: "La prevención de riesgos laborales y la protección de datos de carácter personal. El caso de la empresa "Air Spain"." Revista Información Laboral, núm. 4, 2014.

MUÑOZ RUIZ, A.B.: "Convergencia y divergencia entre los Tribunales del Orden Social y la Agencia Española de Protección de Datos en materia de control informático de la prestación de trabajo (Comentario a las SSTS de 8 de marzo y de 6 de octubre de 2011)", *Revista Española de Derecho del Trabajo,* núm. 156, 2012.

MURILLO DE LA CUEVA, P.L.: "Informática y protección de datos personales" en *Estudios sobre la LO 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*, col.43, Cuadernos y Debates, Ed. Centro de Estudios Constitucionales, 1993.

MURILLO DE LA CUEVA, P.L.: "La construcción del derecho a la autodeterminación informativa", *Revista de Estudios Políticos*, núm.104, 1999.

MURILLO DE LA CUEVA, P.L.: "Las vicisitudes del Derecho de la protección de datos personales", en VV.AA: *La democracia constitucional: estudios en homenaje al profesor Francisco Rubio Llorente.* (vol. I) Centro de Estudios Políticos y Constitucionales, 2003.

MURILLO DE LA CUEVA, P.L.: "Perspectivas del derecho a la autodeterminación informativa" *Revista Indret*, núm. 5, 2007.

MURILLO DE LA CUEVA, P.L.: *El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática"*, Tecnos, 1991.

NAVALPOTRO NAVALPOTRO, Y.: "Ámbito de aplicación de la Ley Orgánica de protección de datos de carácter personal (LOPD)" en ALMUZARA ALMAIDA, C. (coord.): *Estudio práctico sobre la protección de datos de carácter personal*, Lex Nova, 2005.

NAVALPOTRO NAVALPOTRO, Y.: "Inscripción de ficheros", en ALMUZARA ALMAIDA, C. (coord.): *Estudio práctico sobre la protección de datos de carácter personal*, Lex Nova, 2005.

NAVARRO NIETO, F.: "Los reconocimientos médicos como instrumentos de vigilancia de la salud laboral: condicionantes legales y jurisprudenciales" *Revista Doctrinal Aranzadi Social,* núm.11, 2012.

NÚÑEZ-CORTÉS CONTRERAS, P.: "Algunas medidas para favorecer la empleabilidad en la Reforma Laboral 2012", *Actualidad Laboral*, núm. 19, La Ley, 2012.

OLLERO IZARD, M.: *El proceso de captación y selección de personal,* Gestión, 2000.

OPPENHEIM, CH.: "Cloud law and contract negotiation", El profesional de la información, vol. 21, núm. 5, 2012.

OROZCO PARDO, G.: "Los derechos de las personas en la LORTAD", *Informática y Derecho*, UNED, núms.6 y 7, 1994.

OROZCO PARDO, G: "La protección de datos en Derecho español a la luz de la reciente jurisprudencia constitucional", *Actualidad Civil*, núm.1, 2002.

ORTEGA GIMÉNEZ, A.: "El derecho fundamental a la protección de datos de Carácter Personal en España", *AR. Revista de Derecho Informático*, núm. 121, 2008.

ORTÍ VALLEJO, A.: "El nuevo derecho fundamental (y de la personalidad) a la libertad informática (A propósito de la STC 254/1993, de 20 de julio)" *Derecho privado y Constitución*, núm. 2, 1994.

ORTÍ VALLEJO, A.: *Derecho a la intimidad e informática*, Comares, 1994.
ORTIZ LÓPEZ, P.: "Redes Sociales: funcionamiento y tratamiento de información personal", en VV.AA.: *Derecho y Redes Sociales,* Aranzadi, 2013.

PAGALLO, U.: *La tutela della privacy negli stati unitid'America e in Europa*, Giuffre Editore, 2008.

PALACIOS GONZÁLEZ, M.D.: *"El poder de autodeterminación de los datos personales en Internet" IDP, Revista de Derecho, Internet y Política*, núm. 14, 2012.

PALOMAR OLMEDA, A (coord.).:*Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (aprobado por RDLOPD, de 21 de diciembre)*, Aranzadi, 2008.

PALOMAR OLMEDA, A.: "La encrucijada de la regulación de la protección de datos", *Actualidad Jurídica Aranzadi,* núm. 804, 2010.

PALOMEQUE LÓPEZ, M. C.: "Derechos fundamentales generales y relación laboral: los derechos laborales inespecíficos" en VV.AA*: El modelo social en la Constitución Española 1978*, Ministerio de Trabajo e inmigración, Subdirección General de Publicaciones, 2003.

PALOMEQUE LÓPEZ, M.C.: " Ámbito subjetivo y titularidad del derecho de huelga" en BAYLOS GRAU, A.: *Estudios sobre la huelga*, Bomarzo, 2005.

PARDO FALCÓN, J.: "El juicio de indispensabilidad: un avance de los derechos fundamentales en el ámbito laboral", *Temas Laborales*, núm. 39, 1996.

PEDROSA ALQUEZAR, S.: "Confidencialidad y protección de datos en la vigilancia de la salud de los trabajadores: bases para una prevención de calidad" *Revista CEF, Estudios Financieros y de Seguridad Social*, núm. 21, 2004.

PEDROSA ALQUÉZAR, S.: *La vigilancia de la salud en el ámbito laboral*, CES, 2005.

PÉREZ DE LOS COBOS ORIHUEL F; "La reforma laboral: un nuevo marco legal para las empresas de trabajo temporal" *Actualidad Laboral* núm.16, La Ley, 2010.

PÉREZ DE LOS COBOS ORIHUEL, F. Y THIBAULT ARANDA, J.: "PÉREZ DE LOS COBOS ORIHUEL, F.: "El uso sindical de los medios informáticos en la empresa", *Relaciones Laborales*, núm. 1, 2009.

PEREZ DE LOS COBOS, F.: *El derecho social comunitario en el Tratado de la Unión Europea*, Madrid, Civitas, 1994.

PÉREZ DE LOS COBOS Y ORIHUEL, F. Y THIBAULT ARANDA, J.: "El uso laboral del ordenador y la buena fe (a propósito de la STS de 26 de septiembre de 2007, rec. 966/2006)" *Revista Relaciones Laborales,* núm. 1, 2008.

PÉREZ DE VELASCO J.R.: "Protección de datos de carácter personal", *Revista Española de Derecho Internacional*, núm. 27, 2000.
PÉREZ ESPINOSA, F.: "Las empresas de trabajo temporal: a medio camino entre la apertura de los sistemas de colocación y la flexibilización de la mano de obra" en VV.AA.: *La reforma del mercado laboral*, Lex Nova, 1999.

PÉREZ LUÑO, A.E.: "El derecho a la autodeterminación informativa"*,* en *II Jornada de Estudio sobre "Protección de datos y Derechos fundamentales*" Servicios de Estudios del IVAP, 1991.

PÉREZ LUÑO, A.E.: "Informática y libertad. comentario al artículo 18.4 de la Constitución española", *Revista de Estudios Políticos*, núm. 24, 1981.

PÉREZ LUÑO, A.E.*:* "Libertad Informática. Nueva frontera de los derechos fundamentales", *en el vol. de LOSANO, M., La libertad informática y leyes de protección de datos personales, Centro de Estudios Constitucionales, Madrid, 1989.*

PÉREZ LUÑO, A.E.: *La tercera generación de los derechos humanos*, Aranzadi, 2006.

PÉREZ LUÑO, A.E: "El derecho a la autodeterminación informativa"*,* en *II Jornada de Estudio sobre "Protección de datos y Derechos fundamentales*" Servicios de Estudios del IVAP, 1991.

PÉREZ LUÑO. A.E.: *Manual de informática y derecho,* Ariel, 1996.

PÉREZ SÁNCHEZ, C.: "El teletrabajo: ¿Más libertad o una nueva forma de esclavitud para los trabajadores?" *Revista de Derecho, Internet y Politica (UOC)*, núm. 11, 2010.

PÉREZ VELASCO, M.M.: "Los ficheros públicos" en TRONCOSO REIGADA, A. (coord.): *Estudios sobre Administraciones Públicas y Protección de datos personales,* Thomson-Civitas, 2006.

PIÑAR MAÑAS J.L: "*Protección de datos: origen, situación actual y retos de futuro"* en MURILLO DE LA CUEVA*,* P.L.: *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, 2009.

PIÑAR MAÑAS, J.: "Protección de datos y relaciones laborales" en FARRIOLS I SOLA, A: *La protección de datos en los centros de trabajo*, Cinca, 2006.

PIÑAR MAÑAS, J.L.: "Administración Electrónica y protección de datos personales" *Dereito: Revista Xuridica da Universidade de Santiago de Compostela*, núm.1, 2011.

PIÑAR MAÑAS, J.L.: "Concepto de dato de carácter personal" en TRONCOSO REIGADA, A.: *Comentario a la Ley Orgánica de protección de Datos de car*, Thomson-Civitas, 2010.

PIÑAR MAÑAS, J.L.: "Transparencia y protección de datos. Una referencia a la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno" en VV.AA.: *Transparencia, acceso a la información y protección de datos*, Reus, 2014.

PLANAS GÓMEZ, M.: *Gestión Práctica de la Seguridad Social*, CISS, 2007.

PLAZA PENEDÉS, J.: "Aspectos básicos de los derechos fundamentales y la protección de datos de carácter personal en Internet" en VV.AA.: *Derecho y nuevas tecnologías de la información y la comunicación*, Aranzadi, 2013.

PORRET GELABERT, M.: *Manual para la gestión del capital humano en las organizaciones*., ESIC editorial, 2014.

PRIETO GUTIÉRREZ, J.M.: "Objeto y naturaleza jurídica del derecho fundamental de protección de datos", *Boletín del Ministerio de Justicia*, núm.1971-1972, 2004.

PROSSER, W.L.: "Privacy", *California Law Review*, núm.48, 1960.

PULIDO QUECEDO, M.: "¿Numerus clausus o numerus apertus en materia de derechos fundamentales?: el derecho fundamental a la protección de datos", *Repertorio Aranzadi del Tribunal Constitucional*, núm. 20, 2000.

PURCALLA BONILLA, M.A.: "Marcos Jurídicos y experiencias prácticas de Teletrabajo" *Aranzadi Social*, núm.18, 2003.

QUÍLEZ AGREDA, E.: "Datos especialmente protegidos: tratamiento de los ficheros de afiliados de los partidos políticos en los procesos electorales internos: Título II. Principios de la Protección de Datos. Artículo 7.2" en TRONCOSO REIGADA, A.: Comentarios a la Ley Orgánica de Protección de Datos, Thomson-Civitas, 2010.

QUINTERO LIMA, M.G.: "El uso de medios electrónicos, informáticos y telemáticos en relación con los actos de gestión de seguridad social: el sistema de remisión electrónica de datos (sistema red)" *Revista de la contratación electrónica*, núm. 61, 2005.

RABANAL CARBAJO, P.: "Derechos de información de los representantes de los trabajadores. Condiciones económicas precisas de los contratos. Deben comunicarse aun en contra de la voluntad de los trabajadores afectados", *Aranzadi Social*, núm. 14, 2006.

RAMÍREZ MARTÍNEZ, J.M.: "El proceso de colocación: intervencionismo público e iniciativa privada" en ALARCÓN CARACUEL, M.R. (coord.): *La reforma laboral de 1994* , Marcial Pons, 1994.

RAMOS QUINTANA, M.:"Intermediación laboral y empresas de trabajo temporal en la reforma de 2010: la promoción de la intervención privada en el mercado de trabajo", *Revista Relaciones Laborales,* núm. 2, Sección Doctrina, La Ley 2011.

RAY J.E.: "Une loi macédonienne? Etude critique du titre V de la Loi du 31 décembre 1992: Dispositions relatives au recrutement et aux libertés individuelles", *Revista Droit Social*, núm. 2, 1993.

RAZQUIN LIZARRAGA, M.: *La confidencialidad de los datos empresariales en poder de las Administraciones Públicas*, Iustel, 2013.
REMOLINA ANGARITA, N.: "Aproximación constitucional de la protección de datos personales en Latinoamérica" *Revista Internacional de Protección de Datos,* vol. I, 2012.

RIBAGORDA GARNACHO, A.: "La protección de datos personales y la seguridad de la información", *Revista Jurídica de Castilla y León*, núm.16, 2008.

RIBAS, J.: "Actos desleales de los trabajadores usando sistemas informáticos e internet", *Revista Relaciones Laborales*, núm. 2, 2004, pág. 105 y ss.

RODOTA, S.: "Privacy e construzione della sfera privata. Ipotesi e prospettive" *Política del diritto*, núm.4, 1991.

RODRÍGUEZ BEREIJO, A.: "La Carta de los derechos fundamentales de la Unión Europea y la protección de los derechos humanos" en FERNÁNDEZ SOLA, N. (coord.): *Unión Europea y Derechos fundamentales en perspectiva constitucional,* Dykinson,, 2004.

RODRÍGUEZ CARDO, I.: "Pruebas obtenidas a través de detectives privados y derecho a la intimidad del trabajador", *Actualidad Laboral*, núm. 12, 2014.

RODRÍGUEZ ESCANCIANO, S.: "El derecho a la protección de datos personales de los trabajadores como garantía de la libertad sindical" *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 27, 2011.

RODRÍGUEZ ESCANCIANO, S.: "Utilización y control de datos laborales automatizados", *Revista Española de Protección de datos* núm. 2, 2007.
RODRÍGUEZ ESCANCIANO, S.: *La intermediación en el mercado de trabajo: Análisis y propuestas*, Tirant lo Blanch, 2012.

RODRÍGUEZ ESCANCIANO, S: *El derecho a la protección de datos personales de los trabajadores: nuevas perspectivas,* Bomarzo, 2009.

RODRÍGUEZ ESCANCIANO, S; "La potencialidad lesiva de la informática sobre los derechos del trabajador" *Revista Española de Protección de Datos*, núm. 2, 2007.

RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, Tirant lo Blanch, 2015.

RODRÍGUEZ LAINZ, J.L.: "SITEL y principio de proporcionalidad en la intervención de comunicaciones electrónicas" *Diario La Ley*, núm. 7689, 2011.

RODRÍGUEZ PALENCIA, A.: "La protección de datos en el ámbito de la relación jurídico-administrativa", *Anuario de la Facultad de Derecho de la Universidad de Alcalá,* núm. 2, 2009.

RODRÍGUEZ RAMOS, M.J.: *Las elecciones sindicales en la empresa y en los centros de trabajo*, Aranzadi, 2002.

RODRÍGUEZ-PIÑERO ROYO Y DE SOTO RIOJA, S.: "Comentario al art. 11 de la LOLS" en VV.AA.: *La Ley Orgánica de Libertad Sindical. Comentada y con jurisprudencia*, La Ley, 2010.

RODRÍGUEZ-PIÑERO ROYO, M.: "Concepto de empresa de trabajo temporal" en VV.AA.: *Comentario a la Ley de Empresas de Trabajo Temporal*, La Ley, 2009.
RODRÍGUEZ-PIÑERO ROYO, M.: "El nuevo papel de las empresas de trabajo temporal" en VV.AA.: Diez años desde la regularización de las empresas de trabajo temporal, Mergablum (CARL), 2004.

RODRÍGUEZ-PIÑERO ROYO, M.: "Outplacement, head-hunter y otras formas de intervención privada en el mercado de trabajo", en *La reforma del mercado de trabajo y de la seguridad y salud laboral*, Universidad de Granada, 1996.

RODRÍGUEZ-PIÑERO ROYO, M.: *Público y privado en el mercado de trabajo de los 90*, Lección Inaugural Apertura Curso Académico, Universidad de Huelva, 1994.

RODRÍGUEZ-PIÑERO Y BRAVO FERRER, M.: "El deber del empresario de informar al trabajador de sus condiciones de trabajo" *Revista Relaciones Laborales*, núm. 1, 2000.

RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, M.: "Del Statuto dei lavoratori al Estatuto de los trabajadores. Dos experiencias en contraste" en VV.AA.: *El Estatuto de los Trabajadores Italiano veinte años después*, Ministerio de Trabajo y Seguridad Social, 1993.

RODRÍGUEZ–PIÑERO Y BRAVO–FERRER, M.: "El nuevo régimen de las agencias privadas de colocación", *Relaciones Laborales*, núm. 3, 2011.

RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, M.: "Libertad ideológica, contrato de trabajo y objeción de conciencia", *Revista Relaciones Laborales*, núm. 2, 2003.

RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, M.: "No discriminación en las relaciones laborales" en *Comentarios a las Leyes Laborales. El Estatuto de los trabajadores, Tomo IV*, 1983.

RODRÍGUEZ-SAÑUDO GUTIÉRREZ, F. Y ELORZA GUERRERO, F.: "Derechos fundamentales laborales inespecíficos", en CASTIÑEIRA FERNÁNDEZ, J. (coord.):

El derecho del trabajo y de la Seguridad Social en el año 2002: puntos críticos, CARL, Mergablum, 2003.

RODRÍGUEZ-SAÑUDO GUTIÉRREZ, F.: "La transgresión de la buena fe contractual como causa de despido" en VV.AA.: *Cuestiones actuales de Derecho del Trabajo. Estudios ofrecidos por los catedráticos españoles de Derecho del Trabajo al profesor Manuel Alonso Olea*, Ministerio de Trabajo y Seguridad Social, 1990.

ROIG I BATALLA, A.: "La protección de la privacidad: el derecho al honor y la intimidad personal y familiar, y los límites al uso de la informática(arts. 18.1 y 18.4 CE)"en VV.AA.: *Constitución: desarrollo, rasgos de identidad y valoración en el XXV aniversario (1978-2003)*, 2004.

ROIG, A; *Derechos fundamentales y tecnologías de la información y de las comunicaciones*, Bosch, 2010.

ROJAS, P.: *Reclutamiento y selección 2.0: la nueva forma de encontrar talento,* Editorial UOC, 2010.

ROLDÁN MARTÍNEZ, F., Y HERREROS LÓPEZ, J. M.: "El ejercicio de las libertades de expresión e información de los representantes de los trabajadores en la era de Internet", *Actualidad Laboral*, núm. 12, 2009.

ROQUETA BUJ, R.: *Uso y control de los medios tecnológicos de información y comunicación en la empresa,* Tirant lo Blanch, 2005.

ROUDIL, A.: "Le droit du travail au regard de l'informatisation", *Droit Social*, núm. 4, 1981.

RUBÍ NAVARRETE, J.: "Los principios de protección de datos y el reglamento de medidas de seguridad" en VV.AA*.: XIV Encuentros sobre Informática y Derecho: 2000-2001,* Aranzadi, 2001.

RUBÍ NAVARRETE, J.: "Transferencia internacional de datos" en VV.AA.: *XVII Encuentros de Derecho e Informática*, Universidad Pontificia Comillas, 2003.

RUBIO LLORENTE, F.: "Mostrar los derechos sin destruir la Unión", Revista Española de Derecho Constitucional, núm. 64, 2002, pp. 15-18.

RUIZ CARRILLO, A: *Los datos de carácter personal*, Bosch, 1999.

RUIZ MIGUEL, C.: "El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea", en *Revista de Derecho Comunitario Europeo*, núm. 14, 2003.

RUIZ MIGUEL, C.: "La tercera generación de los derechos fundamentales" *Revista de estudios políticos*, núm.72, 1991.

SÁEZ LARA, C: "Espacio y funciones de las empresas de recolocación" *Revista Temas Laborales,* núm. 107, 2010.

SAGARDOY BENGOECHEA, J.A. Y GIL Y GIL, J.L.: "Derechos de información de los representantes de los trabajadores en materia de contratación", *Revista de Trabajo*, núm. 100, 1990.

SAGARGOY DE SIMÓN, I.: "Datos personales, datos profesionales y su tratamiento automatizado", *Revista Relaciones Laborales,* núm. 1, 1995.

SALAS FRANCO, T. Y ARNAU NAVARRO, F.: *Comentarios a la Ley de Prevención de Riesgos Laborales*, Tirant lo Blanch, 1996.

SALAS FRANCO, T: "El derecho a la intimidad del trabajador y a la propia imagen y las nuevas tecnologías de control laboral" en VV.AA: *Trabajo y libertades públicas*, La Ley, 1999.

SALAS PORRAS, M.: *El servicio público de empleo y el proceso jurídico de colocación,* Consejo Andaluz de Relaciones Laborales, 2010.

SALOMON, D.: *Data privacy and security*, Springer, Nueva York, 2003.

SAMPEDRO BURGOS, G.: "Reflexiones sobre la aplicación de la normativa de protección de datos en el ámbito del control del empresario y sistemas de denuncias internas", *Revista General de Derecho del Trabajo y de la Seguridad Social,* núm. 26, 201.

SAN CRISTÓBAL VILLANUEVA, J.M.: "El control laboral del uso del ordenador por parte del empresario: la consolidación del criterio doctrinal iniciado por el Tribunal Supremo. A propósito de la STS 8-03-2011", *Revista del Poder Judicial*, núm. 90, 2011.

SAN JOSÉ, C.: "Les garanties del ciutadan: tutela de drets ARCO i regim sancionador" en MARICARDONA, J. Y VILASAU SOLANA, M.: *El Reglamento de protección de datos de carácter personal. Aspectos claves,* Editorial UOC, 2008.

SAN JUAN GARCÍA, P.: "Nuevas reglas de juego en la protección de datos", *Revista Lex Nova*, núm. 52, 2008.

SAN MARTIN ALCÁZAR, M.T.: "La protección de datos: el nuevo derecho fundamental del siglo XXI", *Revista Jurídica de la Comunidad de Madrid*, núm. 10, 2001.

SAN MARTIN MAZZUCCONI, C. Y SEMPERE NAVARRO, A.: "Sobre el control empresarial de los ordenadores", Revista Doctrinal Aranzadi Social, núm.3, 2012.

SAN MARTÍN MAZZUCCONI, C.: "La vigilancia del estado de salud de los trabajadores: voluntariedad y periodicidad de los reconocimientos médicos" *Revista del Ministerio de Trabajo y Asuntos Sociales*, núm. 53, 2004.

SAN MARTÍN MAZZUCCONI, C.: "Navegar por internet en horas de trabajo... ¿Quién? ¿Yo?", *Revista Doctrinal Aranzadi Social*, núm. 19, 2010.

SÁNCHEZ BRAVO, A: "La Ley orgánica 15/1999, de protección de datos de carácter personal: diez consideraciones en torno a su contenido", *Revista de Estudios Políticos*, núm. 111 (separata), 2001.

SÁNCHEZ BRAVO A*.: La protección del derecho a la libertad informática en la Unión Europea*, Universidad de Sevilla, 1998.

SÁNCHEZ CARAZO, C Y SÁNCHEZ CARAZO, J.M .: *La intimidad y el secreto médico*, Díaz de Santos, 2000.

SÁNCHEZ CARAZO, C.: "La protección de datos personales de las personas vulnerables" *Anuario de la Facultad de Derecho*, núm. 2, 2009.

SÁNCHEZ TORRES, E.: "El derecho a la intimidad del trabajador en la Ley de Prevención de Riesgos Laborales" *Revista Relaciones Laborales*, núm. 2, 1997.

SÁNCHEZ-CARO, J. Y ABELLÁN, F.: *Datos de salud y datos genéticos: su protección en la Unión Europea y en España*, Comares, 2004.

SÁNCHEZ-RODAS NAVARRO, C.: "La orientación e intermediación directa en el empleo", *Revista Temas Laborales*, núm. 125, 2014.

SÁNCHEZ-URÁN AZAÑA, Y.: "Garantía jurisdiccional del derecho a la no discriminación en la relación de trabajo", *Revista del Ministerio de Trabajo y Asuntos Sociales*, núm. extraordinario sobre igualdad efectiva de mujeres y hombres, 2007.

SANFULGENCIO GUTIÉRREZ, J.A.: "¿Es privado el email?: Reflexiones prácticas sobre el uso del correo electrónico en el trabajo y la utilización del ordenador con fines particulares", *El Graduado: Boletín del Ilustre Colegio de Abogados de Madrid*, núm. 37, 2002.

SANGUINETI RAYMOND, W., "Derechos fundamentales del trabajador y poderes empresariales", *Relaciones laborales* núm. 21, 2012.

SANTIAGO REDONDO, K.M.: "Intimidad, secreto de las comunicaciones y protección de datos de carácter personal. El art. 18 CE", *Revista Relaciones Laborales*, núm. 1, 2014.

SANTOS GARCÍA, D.: *Nociones generales dela Ley Orgánica de Protección de datos y su Reglamento*, Tecnos, 2012.

SCIROCCO, A.: "Acceso a documentos y protección de datos personales: la experiencia del Supervisor Europeo de Datos Personales" en TRONCOSO REIGADA, A, (dir).: *Transparencia administrativa y protección de datos personales*, Civitas, 2008.

SEGOVIANO ASTABURUAGA, M.L.: "El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores", *Revista Jurídica de Castilla y León*, núm. 2, 2004.

SELMA PENALVA, A.: "El control de accesos por medio de huella digital y sus repercusiones prácticas sobre el derecho a la intimidad de los trabajadores", *Revista Doctrinal Aranzadi Social*, núm. 2, 2010.

SELMA PENALVA, A: "Los límites de la tolerancia en la utilización del ordenador de la empresa
para fines personales", *Revista Doctrinal Aranzadi Social*, vol. 4, núm.11, 2012.

SELMA PENALVA, A; *"*La transcendencia práctica de la "vinculación ideológica" en las empresas de tendencia en el ámbito de las relaciones de trabajo" *Anales de Derecho*, núm. 26, 2008.

SEMPERE NAVARRO, A. (COORD.): *El contrato de trabajo*, Aranzadi, 2010, vol. I. VV.AA.: *Contratación Laboral*, FC editorial, 2008.

SEMPERE NAVARRO, A.: "Tras el pronunciamiento del Tribunal Supremo ¿cabe controlar el ordenador de los trabajadores?*, Actualidad Jurídica Aranzadi,* núm. 741, 2007.
SEMPERE NAVARRO, A.V. Y SAN MARTÍN MAZZUCCONI, C.: *Nuevas tecnologías y relaciones laborales,* Aranzadi, 2002.

SEMPERE NAVARRO, A.V.: "El trabajo de los minusválidos: Problemas de su regulación", *Tribuna Social*, núm. 91, 1998.

SEMPERE NAVARRO, A.V.: "La existencia de Dios y los trabajadores"*, Actualidad Jurídica Aranzadi,* núm. 77, 2009.

SEMPERE NAVARRO, A.V.: "Sobre las nuevas tecnologías y las relaciones laborales" *Revista Aranzadi Social*, núm.15, 2002.

SEMPERE NAVARRO, A.V; *"*La intermediación laboral en el RDL 3/2012" *Aranzadi Doctrinal* núm. 1, 2012.

SEMPERE NAVARRO, A.V.: "Contrato laboral y tecnologías novedosas", *Actualidad Jurídica Aranzadi* núm. 912, 2015.

SEONE RODRÍGUEZ, J.A.: "De la intimidad genética al derecho a la protección de datos genéticos. La protección ius fundamental de los datos genéticos en el Derecho español (A propósito de las SSTC 290/2000 y 292/200, de 30 de noviembre)", *Revista de Derecho y Genoma Humano*, núm. 17, 2002.

SEPÚLVEDA GÓMEZ, M.: "Los derechos fundamentales inespecíficos a la intimidad y al secreto de las comunicaciones y el uso del correo electrónico en la relación laboral. Límites y contra límites", *Temas Laborales: Revista Andaluza de trabajo y bienestar social*, núm. 122, 2013.

SERRANO PÉREZ, M.M.: *El derecho fundamental a la protección de datos. Derecho español y comparado*, Thomson-Civitas, 2003.

SIERRA HERNÁIZ, E.: "Los sujetos responsables en el marco de las infracciones administrativas en materia de prevención de riesgos laborales" *Tribuna Social: Revista de Seguridad Social y laboral*, núm. 239, 2010.

SOBRINO GONZÁLEZ, G; "Régimen jurídico de las agencias de colocación", *Revista Temas Laborales* núm. 110, 2011.

SOLA, A: *La protección de datos en los centros de trabajo*, Cinca, 2006.

SOLANES, Á. Y CARDONA RUBERT, M.B.: *Protección de Datos Personales y Derechos de los Extranjeros Inmigrantes*, Tirant Lo Blanch, 2005.

SOLAR CALVO, M.P.: "La protección de datos en la Unión Europea: análisis y perspectivas de futuro." *Revista Aranzadi Unión Europea*, núm. 2, 2012.

SOSA CABRERA, S. Y VERANO TACORONTE, D.: "La influencia del teletrabajo en la dirección y gestión de recursos humanos", *Capital Humano: Revista para la integración y desarrollo de los recursos humanos*, núm. 144, 2001.

SOUVIRÓN MORENILLA, J.M.: "En torno a la juridificación del poder informativo del Estado y el control de datos por la Administración", *Revista Vasca de Administración Pública*, núm. 40, 1994.

SUÁREZ DE SÁNCHEZ, A.: "El acceso por el empresario al correo electrónico de los trabajadores", *La Ley*, núm. 1417, 2002.
SUAREZ GONZÁLEZ, F.: "La capacidad para contratar. En torno al art. 7" en VV.AA.: *El estatuto de los trabajadores veinte años después*, núm. 100 (Edic. Especial) *Revista Española de Derecho del Trabajo*, Civitas, 2000.

TALENS VISCONTI, E.: "La vigilancia de la salud del trabajador y el respeto a su intimidad en el supuesto consumo de drogas", *Revista Española de Drogodependencias*, núm. 2, 2013.

TALENS VISCONTI, E.: "La expectativa razonable de confidencialidad como presupuesto de vulneración de derechos fundamentales en la fiscalización informática llevada a cabo por el empresario" *Revista Doctrinal Aranzadi Social*, núm.8, 2013.

TAPIA HERMIDA, A.: "Uso del correo electrónico para transmitir información de naturaleza laboral y sindical a los trabajadores, por las organizaciones sindicales, en los centros de trabajo y durante la jornada laboral", *Revista de Trabajo y Seguridad Social* CEF), núm. 276, 2006.

TARANCÓN PÉREZ, E. Y ROMERO RÓDENAS, M.J.: *Manual de modalidades de contratación laboral*, Bomarzo, 2014.

TASCÓN LÓPEZ, R.: "El lento (pero firme) proceso de decantación de los límites del poder de control empresarial en la era tecnológica", *Revista Doctrinal Aranzadi Social* núm. 17, 2007.

TASCÓN LÓPEZ, R.: "El tratamiento por los representantes de los trabajadores y por las organizaciones sindicales de los datos personales de los trabajadores: entre lo fácticamente posible, lo socialmente conveniente y lo jurídicamente aceptable" *Revista Española de Protección de datos*, núm.1, 2006.

TASCÓN LÓPEZ, R.: "La adopción de códigos tipo en el ámbito laboral para la protección para la protección de datos personales" en GOÑI SEIN, J.L.: *Ética empresarial y códigos de conducta,* La ley, 2011.

TASCÓN LÓPEZ, R.: "La protección de datos de carácter personal de los trabajadores", *Revista Jurídica de Castilla y León*, núm. 16, 2008.

TASCÓN LÓPEZ, R.: "Principios de la protección de datos: consentimiento del afectado. Los ficheros empresariales sobre trabajadores y los derechos de los mismos en el marco de la relación contractual con el empleador" *Estudios y comentarios legislativos Civitas,* 2010.

TASCÓN LÓPEZ, R.: *El tratamiento por la empresa de datos personales de los trabajadores. Análisis del estado de la cuestión.* Thomson- Civitas, 2005.

TÉLLEZ AGUILERA, A.: *Nuevas tecnologías. Intimidad y protección de datos*. Edisofer, 2001.

TELLO DIAZ L; "Intimidad y «extimidad» en las redes sociales. Las demarcaciones éticas de Facebook" *Revista Científica de Educomunicación*, 2013.

TENA TENA, G.: "Los pros y los contras de las empresas de trabajo temporal", *Acciones e investigaciones sociales*, núm. 10, 2000.

TERRADILLOS ORMAETXEA, E.: *Principio de proporcionalidad, Constitución y Derecho del Trabajo,* Tirant lo Blanch, 2004.
TERRADO SÁNCHEZ, F.: "La agencia de protección de datos: regulación orgánica y estatutaria" *Actualidad Informática Aranzadi*, núm.9, 1993.

THIBAULT ARANDA, J. y JURADO SEGOVIA, A.: "Algunas consideraciones en torno al Acuerdo Marco Europeo sobre Teletrabajo" *Revista Temas Laborales,* núm.72, 2003.

THIBAULT ARANDA, J.: "La incidencia de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en el ámbito de las relaciones laborales", *Revista Relaciones Laborales,* núm. 2, 2000.

THIBAULT ARANDA, J.: "La intimidad informática del trabajador. Novedades de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter

personal" en DAVARA RODRÍGUEZ, M.: *Jornadas sobre Informática y Sociedad,* Comillas, Madrid, 2001.

THIBAULT ARANDA, J.: "La vigilancia del uso de internet en la empresa y la protección de datos personales" *Revista Relaciones Laborales*, núm. 1, 2009.

THIBAULT ARANDA, J.: "Relaciones Laborales e Internet" en VV.AA *Principios de Derecho e Internet,* Tirant lo Blanch, 2005.

THIBAULT ARANDA, J.: *Control multimedia de la actividad laboral*, Tirant lo Blanch, 2006.

THIBAULT ARANDA, J.: *El teletrabajo. Análisis jurídico-laboral*, 2001.

THIBAULT ARANDA, J; "*El Derecho Español*" en VV.AA *Tecnología Informática y Privacidad de los Trabajadores,* Aranzadi, 2003.

TOLEDO BAÑEZ, C.: "La protección de los datos personales y las relaciones laborales en España y Francia: Análisis de las recomendaciones dela AEPD y la CNIL como ejercicio de derecho comparado previo a una traducción jurídica", *Revista Crítica de Historia de las Relaciones Laborales y de la Política Social*, núm. 1 y 2, 2010.

TOSCANI GIMÉNEZ, D. Y CALVO MORALES, D*.:* "El uso de internet y el correo electrónico en la empresa: límites y garantías", *Nueva Revista Española de Derecho del Trabajo*, núm. 165, 2014.

TOSCANI GIMÉNEZ, D.: "El nuevo marco legal de los servicios de colocación y empleo. Especial referencia a las agencias privadas de empleo y empresas de trabajo temporal tras la reforma laboral de 2010" *Revista de Trabajo y Seguridad Social,* CEF*,* núm. 335, 2011.

TOSCANI JIMÉNEZ, D.: *Reconocimientos médicos de los trabajadores y su régimen jurídico laboral*, Bomarzo, 2011.

.TRONCOSO REIGADA, A.: "La administración electrónica y la protección de datos" *Revista Jurídica de Castilla y León, 2008*.

TRONCOSO REIGADA, A.: "La Comunicación de datos personales" en VV.AA.: *Comentario a la Ley Orgánica de Protección de datos,* Thomson-Reuters, 2010.

TRONCOSO REIGADA, A.: "Libertad sindical, libertad de empresa y autodeterminación informativa de los trabajadores", en VV.AA.: *La protección de datos de carácter personal en los centros de trabajo,* Cinca, 2006.

TRONCOSO REIGADO A.: *La protección de datos personales: en busca de su equilibrio,* Tirant lo Blanch, 2011.

TÜRK, A.: *La ley francesa de protección de datos de carácter personal*, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion /conferencias/common/pdfs/ConferenciaTURK.pdf.

TUSET DEL PINO, P.: *La contratación de los trabajadores minusválidos*, Aranzadi, 2000.

UGARTE CATALDO, J.: "Derecho de huelga" en VV.AA. *Diccionario internacional de derecho del trabajo y de la seguridad social*, Tirant lo Blanch, 2014.

UNIQUE: "Sobre el uso de las redes sociales y profesionales como fuentes de reclutamiento y selección de personal", *Revista Capital Humano*, núm. 248, 2010.

VALDÉS DAL-RE, F.: "Contrato de puesta a disposición entre empresa de trabajo temporal y empresa usuaria", en VV.AA.: Comentarios a la Ley de Empresas de Trabajo Temporal, La Ley, 2009.

VALDÉS DAL-RÉ, F.: "Cooperación y coordinación entre el Servicio Público Estatal de Empleo y los Servicios Públicos de Empleo Autonómicos", Revista Temas para el debate, núm. 245, 2015.

VALDÉS DAL-RE, F.: "La reforma de la intermediación laboral", *Relaciones Laborales*, núm. 21-22, 2010.

VALDÉS DAL-RE, F.: "Libertad ideológica y contrato de trabajo: una aproximación de Derecho comparado", *Revista Relaciones Laborales*, núm. 2, 2004.

VALDÉS DAL-RE, F.: "Poderes del empresario y derechos de la persona del trabajador", en APARICIO TOVAR, J. Y BAYLOS GRAU, A. (coord.): *Autoridad y democracia en la empresa*, Trotta, Madrid, 1992.

VALERO TORRIJOS, J. y LÓPEZ PELLICER J.A.: "Algunas consideraciones sobre el derecho a la protección de datos personales en la actividad administrativa", *Revista Vasca de Administración Pública*, núm. 59, 2001.

VALERO TORRIJOS, J.: "Implicaciones para la protección de datos de carácter personal de la Administración Electrónica" en VV.AA.: *La protección de datos en la Administración Electrónica*, Aranzadi-Thomson Reuters, 2009.

VALVERDE ASENCIO, A. J.: RL. "Algunas cuestiones sobre el marco normativo del Sistema de Remisión Electrónica de Documentos a la Tesorería General de la Seguridad Social" *Revista Relaciones Laborales*, núm. 1, 2002.

VALVERDE ASENCIO, A.J. "El derecho a la protección de datos en la relación laboral" en VV.AA *Relaciones Laborales y Nuevas Tecnologías*, La Ley 2005.

VELA SÁNCHEZ-MERLO, C; "La privacidad de los datos en las redes sociales", *Revista Española de Protección de Datos,* núm. 5, 2008.

VELEIRO REBOREDO, B*.: Protección de datos de carácter personal y sociedad de la información,* Estudios Jurídicos Boletín Oficial del Estado, 2008.

VIDAL GIL. E*.: "*Los derechos de tercera generación" en MEGÍAS QUIRÓS, J.J. (coord.): *Manual de derechos humanos: los derechos humanos en el siglo XXI*, Aranzadi, 2006.

VIDAL, P.: "La utilización de las cámaras de video vigilancia para fines disciplinarios y de control del trabajo." *Actualidad Jurídica Aranzadi*, núm. 888, 2014.

VILASAU SOLANA, M.: "El fin de la situación de transitoriedad: la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal ya tiene desarrollo reglamentario", *Revista de Internet, Derecho y Política (UOC)*, núm. 7, 2008.

VIZCAÍNO CALDERÓN, V.: *Comentarios a la Ley Orgánica de Protección de Datos*, Civitas, 2000.

VV.AA *La protección de datos en la Gestión de Empresas*, Revista Aranzadi de Derecho y Nuevas Tecnologías. Aranzadi, Pamplona, 2004.

VV.AA.: "Datos perdidos y propiedades psicométricas en los test de personalidad*", Anales de psicología*, núm. 29/1, 2013.

VV.AA.: "La AEPD abre su propia consulta sobre cloud computing*" Diario La Ley*, Nº 7784, 2012.

VV.AA.: "La protección de datos de carácter personal" *Edición digital Aranzadi*, 2014.

VV.AA.: *"*La reforma del mercado de trabajo durante la crisis financiera internacional" *Derecho PUCP*, núm. 68, 2012.

VV.AA.: "Reflexiones en torno a la protección de los datos de carácter personal", *Nuevas Políticas Públicas*. *Anuario para la modernización de las Administraciones Públicas*, Instituto Andaluz de Administración Pública, núm. 1, 2005.

VV.AA.: "Sistema experto para la selección de personal desarrollador de software" *Ingenio Magno,* vol. 4.
VV.AA.: *Comentarios al Estatuto de los Trabajadores*, Lex Nova, 2014.

VV.AA.: *Comentarios al Estatuto de los Trabajadores*, Thomson-Aranzadi, 2003.

VV.AA.: *Derecho del Trabajo*, Tecnos, 2014.

VV.AA.: *Derechos fundamentales inespecíficos y negociación colectiva,* Thomson Reuters, 2011.

VV.AA.: *Guía Técnica y de Buenas Prácticas en Reclutamiento y Selección de Personal*, Colegio Oficial de Psicólogos de Madrid, 2009.

VV.AA.: *Las relaciones laborales y la innovación tecnológica en España*, Fundación 1º de mayo, 2005.

VV.AA.: *Los test de selección de personal: inteligencia–personalidad*, Deusto, 2003.

VV.AA.: *Principios y derechos de la protección de datos de carácter personal. Doctrina de la Agencia de Protección de Datos de la Comunidad de Madrid.* Thomson-Civitas, 2010.

VV.AA.: *Reclutamiento a través de internet: oportunidades y riesgos*, Harvard Deusto Business Review, 2004.

VV.AA.: *Transparencia, acceso a la información pública y buen gobierno: Estudio de la Ley 19/2013, de 9 de diciembre,* Tecnos, 2014.

VV.AA.: *Veinte años de jurisdicción constitucional en España,* Tirant lo Blanch, 2002.

VV.AA: "Escuchas telefónicas a teleoperadoras", *Repertorio de jurisprudencia Aranzadi*, núm.4, 2004.

VV.AA: "La protección de datos en el contexto laboral" en FARRIOLS I SOLA, A. (COORD.): *La protección de datos de carácter personal en los centros de trabajo contexto labora*l. Cinca, 2006.

VV.AA.: "Protección de datos y contrato de trabajo" *Justicia laboral: revista de Derecho del Trabajo y de la Seguridad Social,* núm. 46, 2011.

VV.AA: "Una aproximación para empresas a la Ley Orgánica de Protección de Datos", *Derecom*, núm.15, 2013.

VV.AA: "Vigilar y trabajar: Una aproximación metodológica sobre la intimidad del trabajador como límite de las facultades de vigilancia y control del empresario. A propósito de las SSTCO 98/2000*,* de 10 abril y 186/2000*,* de 10 julio", *Anuario de la Facultad de Derecho de la Universidad de La Coruña,* núm. 5, 2001.

VV.AA.: *Extinción del contrato de trabajo*, Tirant lo Blanch, 2013.

VV.AA.: *Modalidades de extinción del contrato de trabajo: análisis de su régimen jurídico*, Comares, 2014.

VV.AA: "Y la protección de datos en España cumplió veinte años" *Diario La Ley*, núm. 8031, 2013.

VV.AA: *Introducción a la Protección de datos,* Dykinson*,* 2006.

VV.AA: *Manual de selección de personal*, CEP, 2013.

VV.AA; *Código de intermediación laboral*, WoltersKluwer España, 2011.

VV.AA; *Nuevas tecnologías y relaciones laborales,* Aranzadi, 2002.

VVAA; *La protección de datos y sus mundos,* DAPP, 2009.

WESTIN, A.F.: *Privacy and Freedom,* Atheneum, Nueva York, 1970.

ZABIA DE LA MATA, J.: *Protección de datos: Comentarios al Reglamento*, Lex Nova, 2008.

ZAZGNANEAZIZ: "Las agencias de recolocación y los procesos de outplacement: Como aumentar la empleabilidad de los trabajadores y asesorarles en la búsqueda de trabajo", *Revista Capital Humano*, núm. 268, 2012.

ZWERLING, C.: "Current practice and experience in drug and alcohol testing in theworkplace", *Bulletin of Narcotics*, Vol. 45, núm. 2, 1993.

MATERIALES NORMATIVOS.

- Normativa estatal.

- Real Decreto-Ley 17/1977 de 4 de marzo sobre las relaciones de trabajo (BOE núm. de 9 de marzo de 1977).
- Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (BOE núm.115 de 14 de mayo de 1982).
- Ley 2/1985, de 2 de agosto, de Libertad Sindical (BOE núm. 189 de 8 de agosto de 1985).
- Ley 5/1985 de 19 de junio, de régimen Electoral General (BOE núm. 147 de 20 de junio de 1985).
- Ley 2/1991, de 7 de enero, sobre información a los representantes de los trabajadores en materia de contratación (BOE núm. 7 de 8 de enero de 1991).
- Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los datos de carácter personal (BOE núm. 147 de 21 de junio de 1994).
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos (BOE núm.106 de 4 de mayo de 1993).
- Ley 10/1994, de 19 de mayo, sobre medidas urgentes de fomento de la ocupación (BOE núm. 122 de 23 de mayo de 1994).
- Ley 14/1994, de 1 de junio, de empresas de trabajo temporal (BOE núm.131 de 2 de junio de 1994).
- Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (BOE núm. 147 de 20 de junio de 1994).
- Real Decreto Legislativo 1/1994, de 20 de junio, por el que se aprueba el Texto Refundido de la Ley General de la Seguridad Social (BOE núm. 154 de 29 de junio de 1994).
- Real Decreto 735/1995, de 5 de mayo, por el que se legalizaron las agencias de colocación sin fines lucrativos y los servicios integrados para el empleo (BOE núm.109 de 8 de mayo de 1995).
- Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales (BOE núm. 269 de 10 de noviembre de 1995).
- Real Decreto 84/1996, de 26 de enero, por el que se aprueba el Reglamento general sobre inscripción de empresas y afiliación, altas, bajas y variaciones de datos de trabajadores en la Seguridad Social (BOE núm. 50 de 27 de febrero de 1996).
- Real Decreto 39/1997, de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención (BOE núm. 27 de 31 de enero de 1997).
- Real Decreto 575/1997, de 18 de abril, por el que se regulan determinados aspectos de la gestión y control de la prestación económica de la

Seguridad Social por incapacidad temporal (BOE núm. 98 de 24 de abril de 1997).

- Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación (BOE núm. 25 de 29 de enero de 1998).
- Real Decreto 994/1999, de 11 de junio, por el que se aprobó el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal (BOE núm. 151, de 25 de junio de 1999).
- Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal (BOE núm. 298 de 14 de diciembre de 1999).
- Real Decreto Legislativo 5/2000 de 4 de agosto por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones del Orden Social (BOE núm. 189 de 8 de agosto de 2000).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico (BOE núm.166, de 12 de julio, de 2002).
- Ley 58/2003, de 17 de diciembre, General Tributaria (BOE núm. 302 de 18 de Diciembre de 2003).
- Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y de orden social (BOE núm. 313 de 31 de diciembre de 2003).
- Real Decreto 939/2005, de 29 de julio, por el que se aprueba el Reglamento General de Recaudación (BOE núm. 210 de 2 de septiembre de 2005).
- Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas y de modificación parcial de las leyes de los Impuestos sobre Sociedades, sobre la Renta de no Residentes y sobre el Patrimonio (BOE núm. 285 de 29 de noviembre de 2006).
- Ley 42/2006 de 28 de diciembre de 2006, de presupuestos generales del Estado para el año 2007 (BOE núm. 311 de 29 de diciembre de 2006).
- Real Decreto 439/2007, de 30 de marzo, por el que se aprueba el Reglamento del Impuesto sobre la Renta de las Personas Físicas y se modifica el Reglamento de Planes y Fondos de Pensiones, aprobado por Real Decreto 304/2004, de 20 de febrero (BOE núm. 78 de 31 de marzo de 2007).
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (BOE núm. 150 de 23 de junio de 2007).
- Ley 25/2007 de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (BOE núm. 251 de 19 de octubre de 2007).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE núm. 17, de 19 de enero de 2008).
- Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información (BOE núm. 312 de 29 de diciembre de 2007).
- Real Decreto 10/2010, de 16 de junio, de medidas urgentes para la reforma del mercado laboral (BOE núm.147 de 17 de junio de 2010).
- Ley 35/2010, de 17 de septiembre, de medidas urgentes para la reforma del mercado de trabajo (BOE núm.227 de 18 de septiembre de 2010).
- Real Decreto 1796/2010, de 30 de diciembre, por el que se regulan las agencias de colocación (BOE núm. 318 de 31 de diciembre de 2010).

- Real Decreto-Ley 7/2011 de 10 de junio, de medidas urgentes para la reforma de la negociación colectiva (BOE núm.139 de 11 de junio de 2011).
- Real Decreto-Ley 10/2011 de 26 de agosto, de medidas urgentes para la promoción del empleo de los jóvenes, el fomento de la estabilidad en el empleo y el mantenimiento del programa de recualificación profesional de las personas que agoten su protección por desempleo (BOE núm. 208 de 30 de agosto de 2011).
- Ley 36/2011, de 10 de octubre, reguladora de la Jurisdicción Social (BOE núm. 245 de 11 de octubre de 2011).
- Real Decreto-Ley 3/2012, de 10 de febrero, de medidas urgentes para la reforma del mercado laboral (BOE núm.36 de 11 de febrero de 2012).
- Real Decreto 1674/2012, de 14 diciembre, por el que se establecen las bases reguladoras para la concesión de subvenciones públicas destinadas a la financiación de la acción "Tu primer trabajo EURES" (BOE núm. 301 de 15 de diciembre de 2012).
- Orden ESS/484/2013, de 26 de marzo, por la que se regula el Sistema de remisión electrónica de datos en el ámbito de la Seguridad Social (BOE núm. 75 del 28 de marzo de 2013).
- Ley 14/2013, de 27 de septiembre, de apoyo a los emprendedores y su internacionalización (BOE núm. 233 de 28 de septiembre de 2013).
- Resolución de la Dirección General del Servicio Público de Empleo Estatal por la que se anuncia licitación de un acuerdo marco para la selección de agencias de colocación para la colaboración con los Servicios Públicos de Empleo en la inserción en el mercado laboral de personas desempleadas (BOE núm. 193 de 13 de agosto de 2013).
- Real Decreto-Ley 16/2013, de 20 de diciembre, de medidas para favorecer la contratación estable y mejorar la empleabilidad de los trabajadores (BOE núm. 305 de 21 de diciembre de 2013).
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (BOE núm. 295 de 10 de diciembre de 2013).
- Real Decreto-Ley 3/2014, de 28 de Febrero, de medidas urgentes para el fomento del empleo y la contratación indefinida (BOE núm. 52 de 1 de marzo de 2014).
- Ley 1/2014, de 28 de Febrero, para la protección de los trabajadores a tiempo parcial y otras medidas urgentes en el orden económico y social (BOE núm. 52 de 1 de marzo de 2014).
- Real Decreto-Ley 8/2014, de 4 de Julio, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia (BOE núm.163 de 5 de julio de 2014).
- Orden de 26 de septiembre de 2014, por la que se desarrollan los programas de orientación profesional, itinerarios de inserción y acompañamiento a la inserción regulados por el Decreto 85/2003, de 1 de abril (BOE núm. 193 de 2 de octubre de 2014).
- Ley 36/2014, de 26 de diciembre, de Presupuestos Generales del Estado para el año 2015 (BOE núm.315 de 30 de diciembre).
- Orden ESS/1680/2015, de 28 de julio, por la que se desarrolla el Real Decreto 417/2015, de 29 de mayo, por el que se aprueba el Reglamento de las empresas de trabajo temporal (BOE núm. 198 de 8 de agosto de 2015)

- Real Decreto 417/2015, de 29 de mayo, por el que se aprueba el Reglamento de las empresas de trabajo temporal (BOE núm. 147 de 20 de junio de 2015).
- Orden ESS/1187/2015, de 15 de junio, por la que se desarrolla el Real Decreto 625/2014, de 18 de julio, por el que se regulan determinados aspectos de la gestión y control de los procesos por incapacidad temporal en los primeros trescientos sesenta y cinco días de su duración (BOE núm. 147 de 20 de junio de 2015).
- Real Decreto 7/2015, de 16 de enero, por el que se aprueba la Cartera Común de Servicios del Sistema Nacional de Empleo (BOE núm.31 de 5 de febrero de 2015).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (BOE núm. 236, de 2 de octubre de 2015).
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores publicado en BOE núm. 255 de 24 de octubre).
- Real Decreto Legislativo 3/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley de Empleo (BOE núm. 255 de 24 de octubre).

- **Normativa autonómica.**

- Ley 5/2002, de la Agencia Catalana de Protección de Datos (BOE núm. 115 de 14 de mayo de 2002).
- Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos (BOE núm. 279 de 19 de noviembre de 2011).
- Ley 8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas de la Comunidad de Madrid (Boletín Oficial de la Comunidad de Madrid de 29 de diciembre de 2012).
- Ley 1/2014 de, 24 de junio, de Transparencia Pública de Andalucía (BOJA núm. 124 de 30 de Junio de 2014).
- Decreto 434/2015, de 29 de septiembre, por el que se aprueban los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía (BOJA núm. 193 de 2 de octubre de 2015).

- **Normativa Europea.**

- Convenio núm. 88, de 17 de julio de 1948 sobre organización del servicio del empleo, adoptado en San Francisco, 31ª reunión CIT (09 julio 1948). Ratificado por España el 14 de enero de 1960 (BOE núm. 9, de 11 de enero de 1961).
- Constitución Italiana (Constituzione della Repubblica Italiana), de 22 de diciembre de 1947, Gazzetta Ufficiale del 27 diciembre de 1947, nº 298.
- Statuto dei Lavoratori (Legge núm. 300, de 20 de mayo de 1970) publicada en la Gazeta Ufficiale, de 27 de mayo de 1970.

- Instrumento de Gobierno sueco (La constitución sueca está compuesta de cuatro leyes, y la que hace alusión a la protección de datos de carácter personal es la de Instrumento de Gobierno de 1974, disponible en http://www.wipo.int/wipolex/es/.
- Constitución Portuguesa de 1976 (Diario de la República Portuguesa, 25 de abril de 1976) disponible en: https://dre.pt/constituicao-da-republica-portuguesa.
- Loi nº 78-17, du 6 janvier de 1978 relative a l'informatique, aux fichiers et aux libertés (Journal officiel du 7 janvier de 1978).
- Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981 (BOE núm. 274, de 15 de noviembre de 1985).
- Directiva 91/533/CEE, del Consejo, de 14 de octubre de 1991, relativa a la obligación del empresario de informar al trabajador acerca de las condiciones aplicables al contrato de trabajo o a la relación laboral (DOCE nº L 288/32 de 18 octubre de 1991).
- Directiva 95/46/CE
- Tratado de Ámsterdam (DOCE nº C 340, de 10 de noviembre de 1997).
- Directiva Europea 97/66/CE, de 15 de diciembre de 1997, relativa al tratamiento de datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones (DOCE nº. L 024 de 30, de enero de 1998).
- Lei núm. 67/98, de 26 de outubro, de datos personales (Diario de la República I Serie A núm. 247).
- Convenio para la protección de los derechos humanos y de las libertades fundamentales Convenio Europeo de Derechos Humanos (BOE núm. 108 de 6 de mayo de 1999).
- Decisión de la Comisión Europea 2000/520/CE, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América [notificada con el número C (2000) 2441].
- Carta de los Derechos Fundamentales de la Unión Europea (DOCE nº C 364/1 de 18 de diciembre de 2000).
- Reglamento 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos de la Comunidad y sobre la libre circulación de estos datos (DOCE nº L 008, de 12 de enero de 2001).
- Directiva 2002/58/CE, de 12 de julio, relativa al Tratamiento de Datos Personales y Protección de la Intimidad en el sector de las Comunicaciones Electrónicas (DOCE nº L 201, de 31 de julio de 2002).
- Ley federal de protección de datos alemana de 14 de enero de 2003, publicada en BGBI I, S. 66.

- Código de Trabajo francés (Article 1221-6 Code du Travail, aprobado por Loi nº 99/2003, de 27 de agosto (http://www.legifrance.gouv.fr).
- Tratado de Roma, firmado en Roma, el 29 de octubre de 2004 (DOUE nº C 310, 16 de diciembre de 2004).
- Ley 12/2005 de 26 de enero, de protección de datos genéticos en la selección y contratación de trabajadores (Diario de la República núm.18 de 26 de enero de 2005).
- Loi núm. 2005-32, de 18 de enero de 2005, de programmation pour la cohésion sociale (JORF n°15 du 19 janvier 2005).
- Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DOUE nº 105 de 13 de abril de 2006).
- Tratado de Lisboa (DOUE nº C 306, de 17 de diciembre de 2007).
- Lei 7/2009, de 12 de febrero, que aprueba la revisión del Código de Trabajo portugués (Diario de la República 1ª serie- Nº30-12 de febrero de 2009).
- Decisión 2012/733/UE, de 26 de noviembre, relativa a la aplicación del Reglamento de Ejecución (UE) n° 492/2011 del Parlamento Europeo y del Consejo en lo que respecta a la puesta en relación y la compensación de las ofertas y demandas de empleo y el restablecimiento de EURES (DOUE nº L 328/21 de 28 de noviembre de 2012).
- Reglamento 611/2013, de la Comisión Europea, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas (DOUE nº 173, de 26 de junio de 2013).
- Reglamento (UE) núm. 1303/2013 del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013 , por el que se establecen disposiciones comunes relativas al Fondo Europeo de Desarrollo Regional, al Fondo Social Europeo, al Fondo de Cohesión, al Fondo Europeo Agrícola de Desarrollo Rural y al Fondo Europeo Marítimo y de la Pesca, y por el que se establecen disposiciones generales relativas al Fondo Europeo de Desarrollo Regional, al Fondo Social Europeo, al Fondo de Cohesión y al Fondo Europeo Marítimo y de la Pesca, y se deroga el Reglamento (CE) n ° 1083/2006 del Consejo (DOUE L 347/320 de 20 de diciembre de 2013).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE nº L 191/1 de 4 de mayo de 2016).

- **Recomendaciones y Decisiones.**

- Comité consultivo del Convenio nº 108, Estudio sobre la Recomendación nº R (89) 2, sobre la protección de los datos de carácter personal utilizados con fines de empleo y sugerir propuestas para la revisión de la citada Recomendación, de 9 de septiembre de 2011, adoptada por el Consejo de Ministros el 20 de octubre de 1988.
- Consejo de Europa, Comité de Ministros (1989), Recomendación Rec (89)2 del Comité de Ministros a los Estados miembros sobre la protección de los datos de carácter personal utilizados con fines de empleo, de 18 de enero de 1989.
- Recomendación número R (99) 5, de 23 de febrero de 1999, sobre la protección de la vida privada en internet.
- Decisión de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001.
- Decisión de la Comisión Europea 2002/16/CE, de 27 de diciembre de 2001.
- Decisión de la Comisión Europea 2004/915/CE, de 27 de diciembre de 2004.
- Recomendación de la Comisión Europea, de 12 de mayo de 2009, sobre la aplicación de los principios relativos a la protección de datos y la intimidad en las aplicaciones basadas en la identificación por radiofrecuencia (DOUE L 122/47).
- Recomendación CM/Rec (2015) Comité de Ministros del Consejo de Europa sobre el tratamiento de datos personales en el contexto de empleo, de 1 de abril de 2015.

- **Convenios Colectivos.**

- Convenio Colectivo 2003-2005 de la empresa Telefónica.
- Acuerdo entre Barclays y sección sindical de CC.OO de 21 de junio de 2002.
- Convenio Colectivo de Industrias Aderezo, Relleno, Envasado y Exportación de Aceituna de Sevilla (BOP Sevilla de 12 de junio de 2014).
- Convenio Colectivo Provincial de Oficinas y Despachos de Zaragoza (BOP Zamora de 2 de mayo de 2014)

JURISPRUDENCIA.

- **Tribunales supraestatales regionales.**

- **Tribunal de Justicia de la Unión Europea[1070].**

Sentencia del TJUE de 6 de octubre de 2015 (TJCE 2015\324).
Sentencia del TJUE de 30 de mayo de 2014 (Asunto C-342/12, Worten).
Sentencia del TJUE de 13 de mayo de 2014 (Caso Google Spain y Google) (TJCE 2014\85).
Sentencia del TJUE de 8 de abril de 2014 (Asunto C-293/12 y C-594/12) (TJCE 2014\104).
Sentencia del TJUE de 9 de noviembre de 2010 (Asunto *Volkerund Markus Schecke y Hartmut Eifert contra Land Hessen)* (TJCE 2010\334).
Sentencia del TJCE de 6 de noviembre de 2003, (Asunto C-101/01, Dodi Lindqvist) (TJCE 2003\368).
Sentencia del TJCE de 11 de diciembre de 1997 (Asunto C-55/1996 Job centre II) (TJCE 1997\263).
Sentencia del TJCE 23 abril 1991 (Asunto C-41/90 Höfner) (TJCE 1991\180).
Sentencia del TJCE, de 7 de octubre de 1987 (Caso Strack).
Sentencia del TJCE de 14 de mayo de1974 (Caso Nold, Asunto C-4/73)
Sentencia del TJCE de 17 de diciembre de 1970, (Asunto C-11/70).
Sentencia del TJCE de 12 de noviembre de 1969 (Caso Stauder Asunto C-29/69).

- **Tribunal Europeo de Derechos Humanos.**

Sentencia del TEDH de 12 de enero de 2016 (Caso Barbulescu vs Rumania) (JUR\2016\11790).
Sentencia del TEDH 3 abril 2007 (Caso Copland contra Reino Unido) (TEDH 2007\23): Interceptación y registro del ordenador de trabajo y del teléfono sin consentimiento de la afectada.
Sentencia del TEDH 16 de febrero de 2000 (Caso Aman contra Suiza) (TEDH 2000\87): Intromisión en la vida privada. Violación del art. 8.1 del Convenio Europeo de Derechos Humanos.
Sentencia del TEDH 25 de junio de 1997 (Asunto Halford contra el Reino Unido) (TEDH 1997, 37): Escuchas telefónicas del teléfono privado del despacho de la demandante.

- **Tribunales estatales.**

- **Tribunal Constitucional.**

[1070] Hasta la entrada en vigor, el 1 de diciembre de 2009, del Tratado de Lisboa, su denominación era la de Tribunal de Justicia de las Comunidades Europeas. Todas ellas obtenidas de la página web del Tribunal de Justicia de la Unión Europea: curia.europa.eu.

Sentencia del Tribunal Constitucional de 3 de marzo de 2016 (RTC 2016\39).
Sentencia del Tribunal Constitucional de 18 diciembre de 2014 (RTC 2014\211).
Sentencia del Tribunal Constitucional de 10 de octubre de 2013 (BOE núm. 267 de 7 de noviembre de 2013).
Sentencia del Tribunal Constitucional de 7 de octubre de 2013 (RTC 2013\170).
Sentencia del Tribunal Constitucional de 11 de febrero (RTC 2013\29).
Sentencia del Tribunal Constitucional de 17 de diciembre (BOE núm. 19 de 22 de enero de 2013).
Auto del Tribunal Constitucional, de 28 de enero, (RTC 2008\29).
Sentencia del Tribunal Constitucional de 12 de diciembre de 2005 (RTC 2005\326).
Sentencia del Tribunal Constitucional de 7 de noviembre de 2005 (RTC 2005\281).
Sentencia del Tribunal Constitucional de 15 de noviembre de 2004 (RTC 2004/196).
Sentencia del Tribunal Constitucional de 4 de junio de 2001 (BOE núm. 158, de 3 de julio de 2001).
Sentencia del Tribunal Constitucional de 30 de noviembre (RTC 2000\292).
Sentencia del Tribunal Constitucional de 30 de noviembre (RTC 2000\290).
Sentencia del Tribunal Constitucional de 10 de julio (RTC 2000\186).
Sentencia del Tribunal Constitucional de 10 de abril (RTC 2000\98).
Sentencia del Tribunal Constitucional de 8 de noviembre (RTC 1999, 202).
Sentencia del Tribunal Constitucional de 18 de mayo de 1998 (RTC 1998\105).
Sentencia del Tribunal Constitucional de 13 de julio de 1998 (RTC 1998\158).
Sentencia del Tribunal Constitucional de 15 de junio de 1998 (RTC 1998\123).
Sentencia del Tribunal Constitucional de 13 de enero de 1998 (RJ 11/1998).
Sentencia del Tribunal Constitucional de 19 de junio de 1995 (BOE núm. 175 de 24 de julio de 1995).
Sentencia del Tribunal Constitucional de 26 de septiembre (RTC 1995/139).
Sentencia del Tribunal Constitucional de 11 de abril (RTC 1994\99).
Sentencia del Tribunal Constitucional de 22 de abril de 1993 (RTC 1993/142).
Sentencia del Tribunal Constitucional de 20 de julio (RTC 1993\254).
Sentencia del Tribunal Constitucional de 7 de abril de 1983 (RTC 1983/25).
Sentencia del Tribunal Constitucional de 27 de junio (BOE núm.170 de 17 de julio de 1985).
Sentencia del Tribunal Constitucional de 17 de octubre (BOE núm. 268, de 8 de noviembre de 1985).
Sentencia del Tribunal Constitucional de 13 de febrero de 1981 (RTC 1981\5).

- **Audiencia Nacional.**

Sentencia de la Audiencia Nacional de 4 de diciembre de 2015(JUR 2015\306870).
Sentencia de la Audiencia Nacional (Sala de lo Contencioso Administrativo) de 22 de enero de 2014 (JUR 2014\38439).
Sentencia de la Audiencia Nacional de 28 de enero de 2014 (AS 2014\231).
Sentencia de la Audiencia Nacional de 19 de marzo de 2014 (JUR 2014\102121).

Sentencia de la Audiencia Nacional de 12 de junio de 2014 (JUR 2014\193394).
Sentencia de la Audiencia Nacional (Sala de lo Contencioso Administrativo) de 24 de junio de 2014 (RJCA 2014\580).
Sentencia de la Audiencia Nacional de 29 de diciembre de 2014 (RJCA 2015\181).
Sentencia de la Audiencia Nacional de 4 de febrero de 2013 (JUR 2013\61765).
Sentencia de la Audiencia Nacional de 26 de junio de 2012 (RJCA 2012\720).
Sentencia de la Audiencia Nacional, de 15 de octubre de 2012 (JUR 2012\342116).
Sentencia de la Audiencia Nacional, de 25 de octubre de 2012 (JUR 2013\54501).
Sentencia de la Audiencia Nacional de 22 de septiembre de 2011 (RJCA 2011\730).
Sentencia de la Audiencia Nacional de 4 de marzo de 2010 (JUR 2010/90775).
Sentencia de la Audiencia Nacional de 11 de marzo de 2010 (RJCA 2010\238).
Sentencia de la Audiencia Nacional de 12 de julio de 2010 (ROJ SAN 3301/2010).
Sentencia de la Audiencia Nacional de 3 de diciembre de 2010 (JUR 2010\413684).
Sentencia de la Audiencia Nacional de 19 de diciembre de 2007 (JUR 2008\11648).
Sentencia de la Audiencia Nacional de 18 de octubre de 2007 (JUR 2007\346177).
Sentencia de la Audiencia Nacional 160/2006, de 3 de octubre de 2007 (JUR 2007\316013).
Sentencia de la Audiencia Nacional, de 16 de febrero de 2006 (JUR 2006\119381).
Sentencia de la Audiencia Nacional de 25 de mayo de 2006 (JUR\2006\174370).
Sentencia de la Audiencia Nacional, de 18 de diciembre de 2006 (RJCA 2007\99).
Sentencia de la Audiencia Nacional 74/2005 de 12 de julio (AS 2005\2674).
Sentencia de la Audiencia Nacional 52/2005, de 27 de mayo (AS 2005\2728).
Sentencia de la Audiencia Nacional de 27 de abril de 2005 (JUR 2006\196759).
Sentencia de la Audiencia Nacional de 15 de junio de 2005 (JUR 2005\240213).
Sentencia de la Audiencia Nacional de 21 de abril de 2004 (RJCA 2004\809).
Sentencia de la Audiencia Nacional de 19 de mayo de 2004 (JUR 2004\253765).
Sentencia de la Audiencia Nacional de 27 de mayo de 2004 (AS 2004/2726).
Sentencia de la Audiencia Nacional de 9 de junio de 2004(JUR 2004\253577).
Sentencia de la Audiencia Nacional, de 11 de noviembre de 2004 (JUR 2005\232306).
Sentencia de la Audiencia Nacional de 24 de enero de 2003 (JUR 2006\275817).
Sentencias de la Audiencia Nacional de 7 de febrero de 2003 (2006\275713).
Sentencia de la Audiencia Nacional de 15 de octubre de 2003 (JUR 2004\53521).

Sentencia de la Audiencia Nacional, de 8 de marzo de 2002 (JUR\2002\143289).
Sentencias de la Audiencia Nacional de 12 de abril de 2002(PROV 2002, 143466).
Sentencia de la Audiencia Nacional de 10 de mayo de 2002 (PROV 2003, 49667).
Sentencia de la Audiencia Nacional de 14 de junio de 2002 (JUR 2003\49779).
Sentencia de la Audiencia Nacional, de 15 de junio de 2001(JUR 2001\293673).
Sentencia de la Audiencia Nacional de 30 de noviembre de 2001 (ROJ: SAN 7179/2001).

- **Tribunal Supremo.**

Sentencia del Tribunal Supremo de 14 de marzo de 2016 (ROJ: STS 964/2016)
Sentencia del TS de 12 de noviembre de 2015 (RJ 2015\5063).
Sentencia del Tribunal Supremo de 15 de octubre de 2015 (ROJ: STS 4132/2015).
Sentencia del Tribunal Supremo de 21 de septiembre de 2015 (JUR 2015\239514).
Sentencia del Tribunal Supremo de 10 de junio de 2015 (JUR 2015\180919).
Sentencia del Tribunal Supremo de 13 de mayo de 2014 (RJ\2014\3307).
Sentencia del Tribunal Supremo de 8 de abril de 2014 (RJ 2014\4346).
Sentencia Tribunal Supremo de 5 de febrero de 2013 (RJ 2013\928).
Sentencia del Tribunal Supremo de 13 de marzo de 2012 (RJ 2012\4917).
Sentencia del Tribunal Supremo de 16 de diciembre de 2011 (RJ 2012\2832).
Sentencia del Tribunal Supremo de 6 de octubre de 2011 (RJ 2011\7699)
Sentencia del Tribunal Supremo de 8 de marzo de 2011 (RJ 932/2011).
Sentencia del Tribunal Supremo de 27 de octubre de 2010 (RJ 2010\8461).
Sentencia del Tribunal Supremo de 9 de febrero de 2009 (RJ 2009\1620).
Sentencia del Tribunal Supremo de 27 de septiembre de 2007 (RJ 2007\7095).
Sentencia del Tribunal Supremo de 26 de septiembre de 2007 (RJ 7514/2007).
Sentencia del Tribunal Supremo de 2 de julio de 2007 (RJ 2007\6598).
Sentencia del Tribunal Supremo de 18 de diciembre de 2006 (RJ 2007/750).
Sentencia del Tribunal Supremo de 25 de noviembre de 2005 (2006/5925).
Sentencia del Tribunal Supremo de 5 de diciembre de 2003 (RJ 2004\313).
Sentencia del Tribunal Supremo (Sala de lo Civil) de 21 de mayo de 1997 (RJ 1997\4122).
Sentencia del Tribunal Supremo de 19 de julio de 1989 (RJ 1989\5878).

- **Tribunales Superiores de Justicia.**

Sentencia del TSJ de Madrid de 16 de junio de 2015 (AS 2015\1304).

Sentencia del TSJ de Madrid de 10 de junio de 2015 (JUR 2015\178247).
Sentencia del TSJ de Castilla la Mancha de 23 de marzo de 2015 (JUR 2015\95400).
Sentencia del TSJ de Cataluña de 15 de julio de 2014 (JUR 2014\243599).
Sentencia del TSJ de Castilla y León de 10 de junio de 2014 (AS 2014\1619).

Sentencia del TSJ de Cantabria de 18 de junio de 2014 (PROV 2014, 180053).
Sentencia del TSJ de Canarias de 7 de abril de 2014 (AS 2014\2179).
Sentencia del TSJ de Galicia de 17 de enero de 2014 (AS 2014\637)
Sentencia del TSJ de Andalucía de 14 de noviembre de 2013 (AS 2013\2935).
Sentencia del TSJ Madrid de 5 de julio de 2013 (AS 2013\2760).
Sentencia del TSJ de Galicia de 2 de mayo de 2013 (RJCA 2013\603).
Sentencia del TSJ de Extremadura de 5 de febrero de 2013 (AS 2013\246).
Sentencia del TSJ del País Vasco de 17 de abril de 2012 (AS 2012\1676).
Sentencia del TSJ de Madrid de 27 de enero de 2012 (JUR\2012\114977).
Sentencia del TSJ de Madrid, de 4 de noviembre de 2011 (AS 2011\2581).
Sentencia del TSJ de Valencia de 28 de septiembre de 2010 (AS 2011\47).
Sentencia del Tribunal Superior de Justicia de Murcia de 25 de enero de 2010 (AS 165/2010).
Sentencia del TSJ de Cataluña de 18 de enero de 2010 (AS 2010\983).
Sentencia del TSJ de Madrid de 13 de octubre de 2009 (AS 2009\2930).
Sentencia del TSJ de Canarias de 21 de julio de 2009 (JUR 2009\446907).
Sentencia de del TSJ de Asturias, de 6 de febrero de 2009 (AS 2009\1142).
Sentencia del TSJ de Madrid de 5 de noviembre de 2008 (AS 2009\133).
Sentencia del TSJ de Murcia de 3 de julio de 2008 (AS 2009\1031).
Sentencia del TSJ de Madrid de 30 de junio de 2008 (AS 2008\2186).
Sentencia del TSJ Canarias Las Palmas del 23 de febrero de 2006 (JUR 2006\127499).
Sentencia del TSJ de Aragón de 4 de diciembre de 2007(AS 2008\1076).
Sentencia del TSJ de Andalucía de 18 de julio de 2007 (AS 2008\174).
Sentencia del TSJ de Islas Canarias de 17 de julio de 2007(AS 2007\2185).
Sentencia del TSJ Madrid del 27 de junio de 2007 (AS 2007\3037).
Sentencia del TSJ de Cantabria de 18 de enero de 2007 (AS 2007\1030).
Sentencia del TSJ del País Vasco de 16 de mayo de 2006 (AS 2007\1028).
Sentencia del TSJ Cataluña del 13 de mayo de 2005 (JUR 2005\169963).
Sentencia del TSJ de Cataluña de 8 de marzo de 2005 (AS 2005\1367).
Sentencia del TSJ de Madrid de 8 de febrero de 2005 (AS 2005\156).
Sentencia del TSJ de Madrid de 24 de junio de 2004 (AS 2004\2323).
Sentencia del TSJ de Asturias de 30 de abril de 2004 (AS 2004\2112).
Sentencia del TSJ de Castilla la Mancha de 21 de mayo de 2003 (AS 2003\2920).
Sentencia del TSJ de Canarias de 22 de marzo de 2002 (AS 2002\2629).
Sentencia del TSJ de Madrid de 31 de enero de 2002 (AS 2002\916).
Sentencia del TSJ de Castilla y León de 19 de marzo de 2001 (AS 2001\2200).
Sentencia del TSJ de Cataluña de 5 de julio de 2000 (AS 2000\3452).
Sentencia del TSJ de Cataluña de 23 de octubre de 2000 (AS 2000/4536).
Sentencia del TSJ de Andalucía de 6 de abril de 1998 (RJCA 1998\1146).
Sentencia del TSJ de Justicia de Castilla y León de 3 de diciembre de 1996 (AS 1996, 3998).
Sentencia del TSJ de Cantabria de agosto de 1996(AS\1996\2748).

- **Juzgados de Lo Social.**

Sentencia del Juzgado de lo Social de Barcelona de 12 de noviembre de 2014(JUR 2015\185688).

Sentencia núm. 213/2011 de 3 de mayo del Juzgado de lo Social de Almería(AS 2011\1151).

OTRAS FUENTES.

- **AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.**

INFORMES JURÍDICOS DE LA AEPD.

- Informe jurídico 368/2003 de la AEPD.
- Informe jurídico 434/2004 de la AEPD.
- Informe jurídico 513/2004 de la AEPD.
- Informe jurídico 16/2005 de la AEPD.
- Informe Jurídico 78/2005 de la AEPD.
- Informe jurídico 167/2005 de la AEPD.
- Informe jurídico 191/2005 de la AEPD.
- Informe Jurídico 184/2006 de la AEPD.
- Informe jurídico 624/2006 de la AEPD.
- Informe jurídico 0391/2007 de la AEPD.
- Informe jurídico 42/2008 de la AEPD.
- Informe jurídico 78/2008 de la AEPD
- Informe jurídico 82/2008 de la AEPD.
- Informe jurídico 93/2008 de la AEPD.
- Informe jurídico 128/2008 de la AEPD.
- Informe Jurídico 189/2008 de la AEPD.
- Informe jurídico 193/2008 de la AEPD.
- Informe jurídico 336/2008 de la AEPD.
- Informe jurídico 29/2009 de la AEPD.
- Informe jurídico 39/2009 de la AEPD.
- Informe jurídico 0090/2009 de la AEPD.
- Informe jurídico 92/2009 de la AEPD.
- Informe jurídico 271/2009 de la AEPD.
- Informe jurídico 275/2009 de la AEPD.
- Informe jurídico 0324/2009 de la AEPD.
- Informe jurídico 411/2009 de la AEPD.

- Informe jurídico 424/2009 de la AEPD.
- Informe jurídico 488/2009 de la AEPD.
- Informe jurídico 529/2009 de la AEPD.
- Informe jurídico 322/2010 de la AEPD.
- Informe jurídico 340/2010 de la AEPD.
- Informe Jurídico 384/2010 de la AEPD.
- Informe jurídico 0176/2012 de la AEPD.
- Informe jurídico 0077/2013 de la AEPD.
- Informe jurídico 0184/2013 de la AEPD.
- Informe jurídico 54/2014 de la AEPD.
- Informe jurídico 0013/2016 de la AEPD.

RESOLUCIONES Y PROCEDIMIENTOS SANCIONADORES.

- Resolución 681/2004 de la AEPD de 10 de diciembre de 2004.
- Procedimiento Sancionador AEPD PS/00328/2005 de 31 de julio de 2006
- Procedimiento Sancionador AEPD PS/00014/2006, de 7 de julio de 2006
- Resolución 1823/2008 de la AEPD de 9 de febrero de 2009.
- Resolución 00371/2009 de la AEPD de 4 de marzo de 2009.
- Resolución 1547/2009 de la AEPD de 16 de marzo de 2009.
- Resolución de la AEPD R/02714/2009 de 14 de diciembre de 2009.
- Resolución R/01716/2011 de la AEPD de 27 de julio de 2011.

.

OTROS DOCUMENTOS DE LA AEPD.

- Instrucción 1/1998 de la AEPD, de 19 de enero, sobre los derechos de acceso, rectificación, cancelación y oposición (BOE núm. 25 de 29 de enero de 1998).
- Memoria de la Agencia Española Protección de Datos 2001.
- *Selección de personal a través de internet, AEPD, 2005.*
- Instrucción 1/2006, de 8 de noviembre, de la AEPD (BOE núm. 296 de 12 de diciembre de 2006).
- Guía sobre videovigilancia de la AEPD, 2008.

- Guía del responsable del fichero, AEPD, 2008.
- Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, AEPD, 2008.
- Guía de la protección de datos en las relaciones laborales, AEPD, 2009.
- Memoria de la Agencia Española de Protección de Datos de Carácter Personal 2012.
- Orientaciones para prestadores de servicios de cloud computing, AEPD, 2013.
- Nota de prensa AEPD, de 23 de marzo de 2014, disponible en http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/abr_14/140423_NP_Notificacion_quiebras.pdf.

- **GRUPO DE TRABAJO DEL ART. 29.**

- Documento de trabajo, del Grupo del art. 29, relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, de 24 de octubre de 1995, WP 114, Bruselas, de 25 de noviembre de 2005.
- Informe y Recomendaciones, del Grupo del art. 29, sobre telecomunicaciones y la privacidad en las relaciones laborales, de 29 de agosto de 1996.
- Recomendación del Grupo del art. 29 3/97, de 3 de diciembre, sobre el anonimato en internet.
- Recomendación 1/2001, sobre datos de evaluación de los trabajadores adoptada por el Grupo del Artículo 29 el 22 de marzo de 2001
- Recomendación del Grupo del art. 29 2/2001, de 17 de mayo, sobre determinados requisitos para la recogida en línea de datos de carácter personal.
- Dictamen 8/2001 del Grupo del art. 29 sobre el tratamiento de datos de carácter personal en el contexto laboral, WP 48, Bruselas, de 13 de septiembre de 2001.
- Documento de trabajo del Grupo del art. 29 sobre listas negras, de 3 de octubre de 2002.

- Documento de trabajo sobre biometría del Grupo Trabajo del art. 29, adoptado el 1 de agosto de 2003.
- Dictamen 1/2006 sobre la aplicación de las normas de la UE relativas a la protección a programas internos de denuncia de irregularidades en los campos de la contabilidad, controles contables internos, asuntos de auditoría, lucha contra el soborno, delitos bancarios y financieros, adoptados el 1 de febrero de 2006.
- Dictamen 4/2007 del Grupo del art. 29, adoptado el 20 de junio de 2007.
- Dictamen del grupo del art. 29 sobre cuestiones de protección de datos en relación con buscadores, adoptado el 4 de abril de 2008, disponible en: https://www.agpd.es/portalwebAGPD/canal documentación/internacional.
- Dictamen 5/2009 del Grupo del art. 29 sobre las redes sociales en línea, adoptado el 12 de junio de 2009, disponible en http://ec.europa.eu /justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf.
- Dictamen 15/2011 sobre la definición del consentimiento del grupo de Trabajo del art. 29, adoptado el 13 de julio de 2011.
- Documento del Trabajo sobre la Administración en línea del Grupo del art. 29 (WP 73, 10593/02/ES).

- **PÁGINAS WEBS.**

- *http://www.eduardolagaron.com/wp-content/uploads/2011/02/pro teccic3b3n -de-datos-en-el-c3a1mbito-laboral1.pdf.*
- http://www.legaltoday.com/opinion/articulos-de-opinion/sistemas-de-whistleblowing-o-denuncias-anonimas-en-empresas-cuando-espana-navega-en-solitario.
- http://www.juntadeandalucia.es/servicioandaluzdeempleo/web/websae/portal/es/index.
- http://europa.eu/scadplus/constitution/objectives_es.htm#PRINCIPLES.
- https://clientsites.linklaters.com/clients/dataprotected/Pages/Index.aspx.
- http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/Proteccion_de_datos_y_habeas_data.pdf.
- http://www.dlapiperdataprotection.com/#handbook/world-map-section/c1_US /c2_AR.

- https://ec.europa.eu/eures/.
- https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas _prensa /news/2015_10_06-ides-idphp.php.
- http://www.sistemanacionalempleo.es/informacion.html.
- "Estadísticas usuarios redes sociales en España. 2013 (www.concepto.05.com).
- "Cifras y estadísticas de las Redes Sociales 2013" (www.rvillanuevarios.com).
- http://www.redesociales.net/redesprofesionales/
- http://www.sistemanacionalempleo.es/informacion.html.
- http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/es/pdf.
- https://empleate.gob.es/empleo/#/.
- http://www.sistemanacionalempleo.es/AgenciasColocacion_WEB/listadoAgencias.do?Modo= inicio.
- Portal de empleo de la Comunidad de Madrid http://www.madrid.org/cs/.
- Servicio de Ocupación de Cataluña http://www.oficinadetreball.cat.
- Servicio valenciano de Ocupación y Formación http://www.ocupacio.gva.es.
- Servicio público de empleo del Principado de Asturias: http://www.asturias.es/site/trabajastur.
- http://www.sepe.es/contenidos/inicial/sispe/pdf/NOTA_ INFORMATIVA_ SISPE_ 310305.pdf.
- www.infojobs.es.
- www.infoempleo.net.
- www.computrabajo.es.
- www.trabajando.com.
- www.monster.es.
- www.buscojobs.es.
- www.netemplea.es.
- www.computrabajo.es.
- www.indeed.es.
- http://www.interempleo.es/politica-privacidad
- http://www.acpgranada.com/index.php/agencia-de-colocacion

- http://www.dplett.com/ETT-AVI SOLEGAL.pdf.
- Fundación Adecco (http://www.fundacion adecco.es/Home/Home.aspx)
- Fundación Manpower (http://www.fundacionmanpower.org/).
- Fundación Randstad Empleo (http://www.randstad.es/fundacion)

- **CÓDIGOS DE CONDUCTA.**

- Principios de actuación del Grupo Telefónica, disponible en http://www.telefonica.com/es/abouttelefonica/pdf/NuestrosPrincipiosdeActuacion .pdf.
- Código ético de Red Eléctrica, disponible en http://www.ree.es/sites/default/files/03_GOBIERNO_CORPORATIVO/ Documentos/C.
- Código de conducta de Inditex, disponible en http://www.inditex. com/documents/10279/88163/Codigo-de-conducta-y-practicas- responsables .pdf/
- Código de conducta del BBVA (disponible en http://www.bbva.com/TLBB/fbinesp/codigo_conducta_bbva_nuevo.pdf).
- Política de privacidad de UNIQUE INTERIM S.A. (ETT) .
- Política de Privacidad de Accenture España**,** Política de privacidad red social LinkedIn, disponible en https://es.linkedin.com/.
- Política de privacidad de la red social profesional XING, disponible en https:// www.xing.com/privacy.
- Política de privacidad sede electrónica del SEPE, disponible en https://www.sepe.es/contenidos/enlaces_pie/aviso_legal.html.
- Política de privacidad de la red social profesional XING, disponible en https:// www.xing.com/privacy.
- Política de privacidad red social LinkedIn, disponible en https://es.linkedin.com/.

- **OTROS DOCUMENTOS.**

- OIT: *Tratamiento de cuestiones relacionadas con el alcohol y las drogas en el lugar de trabajo.* Repertorio de recomendaciones prácticas de la OIT, Ginebra, 1996.
- OIT: Principios Directivos, Técnicos y Éticos relativos a las vigilancia de la salud de los trabajadores, Ginebra, 1997.
- OIT: Repertorio de recomendaciones prácticas sobre la protección de los datos personales de los trabajadores, Ginebra, octubre, 1997.
- Comisión Europea: Comunicación sobre la dimensión social y del mercado de trabajo de la sociedad de la información, 1997.

- Recomendación número R (99) 5, de 23 de febrero de 1999, sobre la protección de la vida privada en internet.
- Federal Act concerning the Protection of Personal Data (DSG 2000).
- Estrategia de Lisboa (2005-2008), disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:c11325.
- Agencia Europea de Seguridad de las Redes y de la Información (ENISA): *Cuestiones de seguridad y recomendaciones para las redes sociales en línea,* 2007.
- Resolución sobre protección de la privacidad en los servicios de redes sociales, aprobada en la 30ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (Estrasburgo, 15-17 de octubre de 2008).
- Estándares Internacionales sobre protección de datos personales y privacidad aprobados el 9 de noviembre de 2009 en la Conferencia Internacional (Madrid).
- Norma UNE 15713:2010 (Comité Europeo de Normalización), la cual establece el código de buenas prácticas que deberían cumplir las empresas dedicadas a la destrucción confidencial de documentos.
- BOCG 184/090219 núm. D-456 de 8 de octubre de 2010.
- *Guidepour les employeurs et les salaries* 2010, disponible en: www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_employeurs _salaries.pdf. pdf).
- BOCG núm. D-508 de 14 de enero de 2011.
- Documento Estadísticas Osimga.org 2011, disponible en http://www.osimga.org/export/sites/osimga/gl/documentos/d/20111201 _ontsi _redes _sociais.pdf.
- III Estudio Adecco Profesional sobre Intermediación Laboral, diciembre de 2012, disponible en http://www.adecco.es/_data/Notas Prensa/pdf/420.pdf.
- Dictamen núm. 24/2013 de la APDCAT, disponible en http://www.apdcat /media/dictamen/ca_568.pdf.
- Carta de Servicios del SEPE 2014-2017.
- *Agencias de colocación. Espacio Telemático Común*, Ministerio de Empleo y Seguridad Social, 2015, disponible en: http://www.sistemanacionalempleoes/pdf/agencias/instrucciones_envios.pdf.

- Sistema Nacional de Empleo: *Agencias de colocación. Espacio Telemático Común*, Ministerio de Empleo y Seguridad Social, 2015, disponible en: http://www.sistemanacionalempleo .es/pdf/ agencias /instrucciones_envios.pdf.
- Estudio “Telco Trendsfor 2015+” realizado por Strategy&, la consultora estratégica de PwC, disponible en http://www.strategyand.pwc .com/media/file /Telco-Trends-for-2015-eps.pdf.
- Informe regional de ASEMPLEO (Asociación de empresarios dedicados a la gestión de los recursos humanos), disponible en http: //www.asempleo.com/servicio/in formes/Informe%20Regional_ITR13.pdf.